

# HP StorageWorks

Fabric OS 5.0.0 diagnostics and system error  
messages

reference guide

**Legal and notice information**

© Copyright 2005 Hewlett-Packard Development Company, L.P.

© Copyright 2005 Brocade Communications Systems, Incorporated.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Windows® is a U.S. registered trademark of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Linux® is a U.S. registered trademark of Linus Torvalds.

Fabric OS 5.0.0 diagnostics and system error messages reference guide

# Contents

About this guide . . . . .	19
Intended audience . . . . .	19
Related documentation . . . . .	19
Document conventions and symbols . . . . .	20
HP technical support . . . . .	21
HP Storage web site. . . . .	21
HP authorized reseller . . . . .	21
1 Introduction to system messages . . . . .	23
Changes for this release of Fabric OS . . . . .	23
Changes to this guide for OS v5.0.0 . . . . .	24
ZONE audit messages . . . . .	24
Message severity levels . . . . .	29
Overview of the system messages . . . . .	29
System message log (RASLog) . . . . .	30
Security audit logging . . . . .	30
Dual-CP systems. . . . .	31
System logging daemon . . . . .	31
Port logs . . . . .	31
Panic dump and core dump files . . . . .	31
Trace dumps . . . . .	32
The supportSave command . . . . .	32
System console . . . . .	32
Viewing and configuring the system message logs . . . . .	32
Reading a system message . . . . .	34
Example system message . . . . .	34
Viewing system messages from Advanced Web Tools . . . . .	35
Dumping the system messages. . . . .	36
Viewing the system messages with page breaks . . . . .	36
Clearing the system message log . . . . .	37
Responding to a system message . . . . .	37
Looking up a system message . . . . .	37
Gathering information about the problem . . . . .	37
System module descriptions . . . . .	38
2 Messages. . . . .	47
Authentication error messages . . . . .	47
AUTH-1001 . . . . .	47
AUTH-1002 . . . . .	47
AUTH-1003 . . . . .	48
AUTH-1004 . . . . .	48
AUTH-1005 . . . . .	48
AUTH-1006 . . . . .	49
AUTH-1007 . . . . .	49
AUTH-1008 . . . . .	50
AUTH-1010 . . . . .	50
AUTH-1011 . . . . .	50
AUTH-1012 . . . . .	51
AUTH-1013 . . . . .	51
AUTH-1014 . . . . .	52
AUTH-1017 . . . . .	52

AUTH-1018	53
AUTH-1020	53
AUTH-1022	54
AUTH-1023	54
AUTH-1025	55
AUTH-1027	55
AUTH-1028	56
AUTH-1029	56
AUTH-1030	57
AUTH-1031	57
AUTH-1032	58
AUTH-1033	58
AUTH-1034	59
AUTH-1035	59
AUTH-1036	60
AUTH-1037	60
AUTH-1038	61
Blade error messages	61
BL-1000	61
BL-1001	62
BL-1002	62
BL-1003	63
BL-1004	63
BL-1006	64
BL-1007	64
BL-1008	65
BL-1009	65
BL-1010	66
BL-1011	66
BL-1012	67
BL-1013	67
BL-1014	68
BL-1015	68
BL-1016	69
Bloom error messages	69
BLL-1000	69
Core edge routing module error messages	71
CER-1001	71
Environment monitor error messages	71
EM-1001	71
EM-1002	72
EM-1003	72
EM-1004	73
EM-1005	74
EM-1006	75
EM-1007	75
EM-1008	76
EM-1009	76
EM-1010	77
EM-1011	77
EM-1012	77
EM-1013	78
EM-1014	79
EM-1015	80
EM-1016	80
EM-1017	80
EM-1028	81
EM-1029	82
EM-1031	82

EM-1033	83
EM-1034	83
EM-1036	84
EM-1041	85
EM-1042	86
EM-1043	86
EM-1044	87
EM-1045	87
EM-1046	88
EM-1047	88
EM-1048	89
EM-1049	89
EM-1050	90
EM-1051	91
EM-1052	91
EM-1053	92
EM-1055	93
EM-1056	93
Event management module error messages	94
EVMD-1001	94
Fabric error messages	94
FABR-1001	94
FABR-1002	95
FABR-1003	95
FABR-1004	96
FABR-1005	96
FABR-1006	97
FABR-1007	97
FABR-1008	98
FABR-1009	98
FABR-1010	99
FABR-1011	99
FABR-1012	99
FABR-1013	100
FABR-1014	100
FABR-1015	101
FABR-1018	101
FABR-1019	102
FABR-1020	102
FABR-1021	103
FABR-1022	103
FABR-1023	103
FABR-1024	104
FABR-1029	104
Fabric OS system driver module error messages	105
FABS-1001	105
FABS-1002	105
FABS-1004	106
FABS-1005	106
FABS-1006	107
FABS-1007	107
FABS-1008	108
FABS-1009	108
FABS-1010	108
Fibre Channel miscellaneous error messages	109
FCMC-1001	109
Fibre Channel protocol daemon error messages	109
FCPD-1001	109
FCPD-1002	110

FCPD-1003 . . . . .	110
Fibre Channel physical layer error messages . . . . .	111
FCPH-1001 . . . . .	111
Fabric OS I/O kernel library module error messages . . . . .	111
FKLB-1001 . . . . .	111
FLOOD error messages . . . . .	112
FLOD-1001 . . . . .	112
FLOD-1003 . . . . .	112
FLOD-1004 . . . . .	112
FLOD-1005 . . . . .	113
FLOD-1006 . . . . .	113
Fabric shortest path first error messages . . . . .	114
FSPF-1001 . . . . .	114
FSPF-1002 . . . . .	114
FSPF-1003 . . . . .	114
FSPF-1005 . . . . .	115
FSPF-1006 . . . . .	115
Fabric OS state synchronization framework error messages . . . . .	116
FSS-1001 . . . . .	116
FSS-1002 . . . . .	116
FSS-1003 . . . . .	117
FSS-1004 . . . . .	117
FSS-1005 . . . . .	117
FSS-1006 . . . . .	118
Fabric OS state synchronization management module error messages . . . . .	118
FSSM-1002 . . . . .	118
FSSM-1003 . . . . .	119
FSSM-1004 . . . . .	119
Fabric Watch module error messages . . . . .	120
FW-1001 . . . . .	120
FW-1002 . . . . .	120
FW-1003 . . . . .	121
FW-1004 . . . . .	121
FW-1005 . . . . .	121
FW-1006 . . . . .	122
FW-1007 . . . . .	122
FW-1008 . . . . .	123
FW-1009 . . . . .	123
FW-1010 . . . . .	124
FW-1011 . . . . .	124
FW-1012 . . . . .	124
FW-1033 . . . . .	125
FW-1034 . . . . .	125
FW-1035 . . . . .	126
FW-1036 . . . . .	126
FW-1037 . . . . .	126
FW-1038 . . . . .	127
FW-1039 . . . . .	127
FW-1040 . . . . .	128
FW-1041 . . . . .	128
FW-1042 . . . . .	128
FW-1043 . . . . .	129
FW-1044 . . . . .	129
FW-1045 . . . . .	130
FW-1046 . . . . .	130
FW-1047 . . . . .	131
FW-1048 . . . . .	131
FW-1049 . . . . .	131
FW-1050 . . . . .	132

FW-1051	132
FW-1052	133
FW-1113	133
FW-1114	133
FW-1115	134
FW-1116	134
FW-1117	135
FW-1118	135
FW-1119	136
FW-1120	136
FW-1121	137
FW-1122	137
FW-1123	138
FW-1124	138
FW-1125	138
FW-1126	139
FW-1127	140
FW-1128	140
FW-1129	141
FW-1130	141
FW-1131	142
FW-1132	142
FW-1133	142
FW-1134	143
FW-1135	143
FW-1136	144
FW-1137	144
FW-1138	144
FW-1139	145
FW-1140	145
FW-1141	146
FW-1142	146
FW-1143	146
FW-1144	147
FW-1160	147
FW-1161	148
FW-1162	148
FW-1163	149
FW-1164	149
FW-1165	150
FW-1166	150
FW-1167	151
FW-1168	151
FW-1169	151
FW-1170	152
FW-1171	152
FW-1172	153
FW-1173	153
FW-1174	154
FW-1175	154
FW-1176	154
FW-1177	155
FW-1178	155
FW-1179	156
FW-1180	156
FW-1181	157
FW-1182	157
FW-1183	157
FW-1184	158

FW-1185	158
FW-1186	159
FW-1187	159
FW-1188	160
FW-1189	160
FW-1190	160
FW-1191	161
FW-1192	161
FW-1193	162
FW-1194	162
FW-1195	163
FW-1216	164
FW-1217	164
FW-1218	165
FW-1219	165
FW-1240	166
FW-1241	166
FW-1242	167
FW-1243	167
FW-1244	168
FW-1245	168
FW-1246	168
FW-1247	169
FW-1248	169
FW-1249	170
FW-1250	170
FW-1251	171
FW-1272	171
FW-1273	171
FW-1274	172
FW-1275	172
FW-1296	173
FW-1297	173
FW-1298	174
FW-1299	174
FW-1300	175
FW-1301	175
FW-1302	175
FW-1303	176
FW-1304	176
FW-1305	177
FW-1306	177
FW-1307	178
FW-1308	178
FW-1309	178
FW-1310	179
FW-1311	179
FW-1312	180
FW-1313	180
FW-1314	180
FW-1315	181
FW-1316	181
FW-1317	182
FW-1318	182
FW-1319	182
FW-1320	183
FW-1321	183
FW-1322	184
FW-1323	184



FW-1324	185
FW-1325	185
FW-1326	185
FW-1327	186
FW-1328	186
FW-1329	187
FW-1330	187
FW-1331	188
FW-1332	188
FW-1333	188
FW-1334	189
FW-1335	189
FW-1336	190
FW-1337	190
FW-1338	191
FW-1339	191
FW-1340	192
FW-1341	192
FW-1342	192
FW-1343	193
FW-1344	193
FW-1345	194
FW-1346	194
FW-1347	195
FW-1348	195
FW-1349	196
FW-1350	196
FW-1351	197
FW-1352	197
FW-1353	198
FW-1354	198
FW-1355	199
FW-1356	199
FW-1357	200
FW-1358	200
FW-1359	201
FW-1360	201
FW-1361	201
FW-1362	202
FW-1363	202
FW-1364	203
FW-1365	203
FW-1366	203
FW-1367	204
FW-1368	204
FW-1369	205
FW-1370	205
FW-1371	206
FW-1372	206
FW-1373	207
FW-1374	207
FW-1375	208
FW-1376	208
FW-1377	209
FW-1378	209
FW-1379	210
FW-1400	210
FW-1401	211
FW-1402	211

FW-1403	211
FW-1424	212
FW-1425	212
FW-1426	213
FW-1427	213
FW-1428	213
FW-1429	214
FW-1430	214
FW-1431	215
FW-1432	215
FW-1433	215
FW-1434	216
FW-1435	216
FW-1436	217
FW-1437	217
FW-1438	218
FW-1439	218
FW-1440	218
FW-1441	219
FW-1442	219
FW-1443	220
FW-1444	220
High-availability management error messages	220
HAM-1001	220
HAM-1002	221
HAM-1004	221
HAM-1005	222
High-availability management kernel module error messages	222
HAMK-1001	222
HAMK-1002	223
HAMK-1003	223
Hardware independent layer error messages	224
HIL-1101	224
HIL-1102	224
HIL-1103	224
HIL-1104	225
HIL-1105	225
HIL-1106	226
HIL-1107	226
HIL-1108	227
HIL-1201	227
HIL-1202	228
HIL-1203	228
HIL-1204	229
HIL-1205	229
HIL-1206	230
HIL-1301	230
HIL-1302	230
HIL-1303	231
HIL-1304	231
HIL-1305	232
HIL-1306	232
HIL-1307	232
HIL-1308	233
HIL-1309	233
HIL-1401	233
HIL-1402	234
HIL-1403	234
HIL-1404	234

HIL-1501	235
HIL-1502	235
HIL-1503	236
HIL-1504	236
HIL-1505	237
HIL-1506	237
HIL-1507	238
HIL-1508	238
HIL-1509	239
HIL-1601	239
HIL-1602	240
HELLO protocol error messages	240
HLO-1001	240
HLO-1002	241
HLO-1003	241
Health monitor error messages	242
HMON-1001	242
Hypertext transfer protocol error messages	242
HTTP-1001	242
Kernel software watchdog error messages	243
KSWD-1003	243
Kernel RAS trace module error messages	243
KTRC-1001	243
KTRC-1002	243
KTRC-1003	244
KTRC-1004	244
RASLog subsystem error messages	245
LOG-1000	245
LOG-1001	245
LOG-1002	245
Link state database error messages	246
LSDB-1001	246
LSDB-1002	246
LSDB-1003	247
LSDB-1004	247
Multicast path error messages	248
MPTH-1001	248
MPTH-1002	248
MPTH-1003	248
Message queue error messages	249
MQ-1004	249
Management service error messages	250
MS-1001	250
MS-1002	250
MS-1003	251
MS-1004	252
MS-1005	252
MS-1006	253
MS-1007	253
MS-1008	254
MS-1021	254
Neighboring switch finite state machine error messages	255
NBFS-1001	255
NBFS-1002	255
NBFS-1003	256
Simple name server module error messages	257
NS-1001	257
NS-1002	257
NS-1003	258

NS-1004 . . . . .	258
Parity data manager error messages . . . . .	259
PDM-1001 . . . . .	259
PDM-1002 . . . . .	259
PDM-1003 . . . . .	259
PDM-1004 . . . . .	260
PDM-1005 . . . . .	260
PDM-1006 . . . . .	261
PDM-1007 . . . . .	261
PDM-1008 . . . . .	262
PDM-1009 . . . . .	262
PDM-1010 . . . . .	262
PDM-1011 . . . . .	263
PDM-1012 . . . . .	263
PDM-1013 . . . . .	264
PDM-1014 . . . . .	264
PDM-1017 . . . . .	264
PDM-1019 . . . . .	265
PDM-1020 . . . . .	265
PDM-1021 . . . . .	266
Panic dump trace error messages . . . . .	266
PDTR-1001 . . . . .	266
PDTR-1002 . . . . .	267
PLAT error messages . . . . .	267
PLAT-1000 . . . . .	267
Port error messages . . . . .	268
PORT-1003 . . . . .	268
PORT-1004 . . . . .	268
Performance server error messages . . . . .	269
PS-1000 . . . . .	269
PS-1001 . . . . .	269
PS-1002 . . . . .	269
PS-1003 . . . . .	270
PS-1004 . . . . .	270
PS-1005 . . . . .	271
Portswap feature error messages . . . . .	271
PSWP-1001 . . . . .	271
PSWP-1002 . . . . .	271
PSWP-1003 . . . . .	272
PSWP-1004 . . . . .	272
Reliable commit service error messages . . . . .	273
RCS-1001 . . . . .	273
RCS-1002 . . . . .	273
RCS-1003 . . . . .	273
RCS-1004 . . . . .	274
RCS-1005 . . . . .	274
RCS-1006 . . . . .	275
Remote procedure call error messages . . . . .	275
RPCD-1001 . . . . .	275
RPCD-1002 . . . . .	276
RPCD-1003 . . . . .	276
RPCD-1004 . . . . .	276
RPCD-1005 . . . . .	277
RPCD-1006 . . . . .	277
RPCD-1007 . . . . .	278
Reliable transport write and read error messages . . . . .	278
RTWR-1001 . . . . .	278
RTWR-1002 . . . . .	278
State change notification error messages . . . . .	279

SCN-1001 .....	279
Security error messages .....	280
SEC-1001 .....	280
SEC-1002 .....	281
SEC-1003 .....	281
SEC-1005 .....	282
SEC-1006 .....	282
SEC-1007 .....	283
SEC-1008 .....	283
SEC-1009 .....	283
SEC-1016 .....	284
SEC-1022 .....	284
SEC-1024 .....	285
SEC-1025 .....	285
SEC-1026 .....	285
SEC-1028 .....	286
SEC-1029 .....	286
SEC-1030 .....	287
SEC-1031 .....	287
SEC-1032 .....	288
SEC-1033 .....	288
SEC-1034 .....	288
SEC-1035 .....	289
SEC-1036 .....	289
SEC-1037 .....	290
SEC-1038 .....	290
SEC-1040 .....	291
SEC-1041 .....	291
SEC-1042 .....	291
SEC-1043 .....	292
SEC-1044 .....	292
SEC-1045 .....	293
SEC-1046 .....	293
SEC-1049 .....	293
SEC-1050 .....	294
SEC-1051 .....	294
SEC-1052 .....	295
SEC-1053 .....	295
SEC-1054 .....	296
SEC-1055 .....	296
SEC-1056 .....	297
SEC-1057 .....	297
SEC-1059 .....	297
SEC-1062 .....	298
SEC-1063 .....	298
SEC-1064 .....	299
SEC-1065 .....	299
SEC-1069 .....	299
SEC-1071 .....	300
SEC-1072 .....	300
SEC-1073 .....	301
SEC-1074 .....	301
SEC-1075 .....	301
SEC-1076 .....	302
SEC-1077 .....	302
SEC-1078 .....	303
SEC-1079 .....	303
SEC-1080 .....	303
SEC-1081 .....	304

SEC-1082.	304
SEC-1083.	305
SEC-1084.	305
SEC-1085.	306
SEC-1086.	306
SEC-1088.	306
SEC-1089.	307
SEC-1090.	307
SEC-1091.	308
SEC-1092.	308
SEC-1093.	309
SEC-1094.	309
SEC-1095.	309
SEC-1096.	310
SEC-1097.	310
SEC-1098.	311
SEC-1099.	311
SEC-1100.	311
SEC-1101.	312
SEC-1102.	312
SEC-1104.	313
SEC-1105.	313
SEC-1106.	314
SEC-1107.	314
SEC-1108.	314
SEC-1110.	315
SEC-1111.	315
SEC-1112.	316
SEC-1115.	316
SEC-1116.	316
SEC-1117.	317
SEC-1118.	317
SEC-1119.	318
SEC-1121.	318
SEC-1122.	318
SEC-1123.	319
SEC-1124.	319
SEC-1126.	320
SEC-1130.	320
SEC-1135.	320
SEC-1136.	321
SEC-1137.	321
SEC-1138.	322
SEC-1139.	322
SEC-1142.	323
SEC-1145.	323
SEC-1146.	324
SEC-1153.	324
SEC-1154.	324
SEC-1155.	325
SEC-1156.	325
SEC-1157.	326
SEC-1158.	326
SEC-1159.	326
SEC-1160.	327
SEC-1163.	327
SEC-1164.	328
SEC-1165.	328
SEC-1166.	328

SEC-1167	329
SEC-1168	329
SEC-1170	330
SEC-1171	330
SEC-1172	331
SEC-1173	331
SEC-1174	331
SEC-1175	332
SEC-1176	332
SEC-1180	333
SEC-1181	333
SEC-1182	333
SEC-1183	334
SEC-1184	334
SEC-1185	334
SEC-1186	335
SEC-1187	335
SEC-1188	336
SEC-1189	336
SEC-1190	337
SEC-1191	337
SEC-1192	338
SEC-1193	338
SEC-1194	338
SEC-1195	339
SEC-1196	339
SEC-1197	340
SEC-1198	340
SEC-1199	341
SEC-1200	341
SEC-1201	342
SEC-1202	342
SEC-1250	343
SEC-1251	343
SEC-1253	343
SEC-1300	344
SEC-1301	344
SEC-1302	345
SEC-1303	345
SEC-1304	345
SEC-1305	346
SEC-1306	346
SEC-1307	347
SEC-1308	347
SEC-3001	348
SEC-3002	348
SEC-3003	349
SEC-3004	349
SEC-3005	350
SEC-3006	350
SEC-3007	351
SEC-3008	351
SEC-3009	351
SEC-3010	352
SEC-3011	352
SEC-3012	353
SEC-3013	353
SEC-3014	354
SEC-3015	354

SEC-3016 . . . . .	354
SEC-3017 . . . . .	355
Simple network management protocol error messages . . . . .	355
SNMP-1001 . . . . .	355
SNMP-1002 . . . . .	356
SNMP-1003 . . . . .	356
SNMP-1004 . . . . .	357
SupportSave command error messages . . . . .	357
SS-1000 . . . . .	357
SS-1001 . . . . .	357
Software upgrade library error messages . . . . .	358
SULB-1001 . . . . .	358
SULB-1002 . . . . .	358
SULB-1003 . . . . .	359
SULB-1005 . . . . .	359
SULB-1006 . . . . .	359
SULB-1007 . . . . .	360
SULB-1008 . . . . .	360
SULB-1009 . . . . .	361
SULB-1010 . . . . .	367
Switch driver module error messages . . . . .	367
SWCH-1001 . . . . .	367
SWCH-1002 . . . . .	368
SWCH-1003 . . . . .	368
SWCH-1004 . . . . .	369
SWCH-1005 . . . . .	369
System controller error messages . . . . .	370
SYSC-1001 . . . . .	370
SYSC-1002 . . . . .	370
General system error messages . . . . .	371
SYSM-1001 . . . . .	371
SYSM-1002 . . . . .	371
SYSM-1003 . . . . .	371
SYSM-1004 . . . . .	372
RAS trace error messages . . . . .	372
TRCE-1001 . . . . .	372
TRCE-1002 . . . . .	373
TRCE-1003 . . . . .	373
TRCE-1004 . . . . .	374
TRCE-1005 . . . . .	374
TRCE-1006 . . . . .	375
TRCE-1007 . . . . .	375
TRCE-1008 . . . . .	375
TRCE-100 . . . . .	376
TRCE-1010 . . . . .	376
TRCE-1011 . . . . .	377
Track change feature error messages . . . . .	377
TRCK-1001 . . . . .	377
TRCK-1002 . . . . .	378
TRCK-1003 . . . . .	378
TRCK-1004 . . . . .	378
TRCK-1005 . . . . .	379
TRCK-1006 . . . . .	379
Time service error messages . . . . .	380
TS-1001 . . . . .	380
TS-1002 . . . . .	380
TS-1006 . . . . .	381
Unicast error messages . . . . .	381
UCST-1003 . . . . .	381



UCST-1007	382
UPATH error messages	382
UPTH-1001	382
User space software watchdog error messages	383
USWD-1006	383
Web Tools error messages	383
WEBD-1001	383
WEBD-1002	384
WEBD-1003	384
WEBD-1004	384
WEBD-1005	385
WEBD-1006	385
WEBD-1007	385
Zone library module error messages	386
ZOLB-1001	386
Zone module error messages	386
ZONE-1002	386
ZONE-1003	387
ZONE-1004	387
ZONE-1005	388
ZONE-1006	388
ZONE-1007	389
ZONE-1008	389
ZONE-1010	390
ZONE-1012	390
ZONE-1013	390
ZONE-1014	391
ZONE-1015	391
ZONE-1017	391
ZONE-1018	392
ZONE-1019	392
ZONE-1022	393
ZONE-1023	393
ZONE-1024	394
ZONE-1026	394
ZONE-1027	394
ZONE-1028	395
ZONE-1029	396
ZONE-1030	396

Glossary	397
----------	-----

Index	417
-------	-----

## Tables

1 Document conventions	20
2 Message severity levels	29
3 Commands to view and configure system logs	32
4 Error message field description	34
5 System module descriptions	38
6 Upgrade messages and code values	366
7 Upgrade state and code values	371



# About this guide

This document provides information to assist fabric administrators in using the web-based graphical user interface to monitor and modify their HP StorageWorks switch fabrics.

This preface discusses the following topics:

- [Intended audience](#), page 19
- [Related documentation](#), page 19
- [Document conventions and symbols](#), page 20
- [HP technical support](#), page 21

---

## Intended audience

This reference guide is intended for systems administrators and technicians experienced with networking, Fibre Channel, and Storage Area Network (SAN) technologies.

---

## Related documentation

Documentation, including white papers and best practices documents, is available via the HP website. Please go to:

<http://www.hp.com/country/us/eng/prodserv/storage.html>

To access 4.x related documents:

1. Locate the **Networked storage** section of the web page.
2. Under **Networked storage**, go to the **By type** subsection.
3. Click **SAN infrastructure**. The SAN infrastructure page displays.
4. Locate the **Fibre Channel Switches** section.

Locate the **B-Series Fabric** subsection, and then go to the appropriate subsection, such as **Enterprise Class** for the SAN Director 2/128.

To access 4.x documents (such as this document), select the appropriate product, for example **SAN Director 2/128 & 2/128 Power Pack** or **Core Switch 2/64 & Core Switch 2/64 Power Pack**.

The switch overview page displays.

5. Go to the **Product information** section, located on the far right side of the web page.
6. Click **Technical documents**.
7. Follow the onscreen instructions to download the applicable documents.

# Document conventions and symbols

**Table 1** Document conventions

Convention	Element
Medium blue text: <a href="#">Figure 1</a>	Cross-reference links and e-mail addresses
Medium blue, underlined text ( <a href="http://www.hp.com">http://www.hp.com</a> )	Web site addresses
<b>Bold font</b>	<ul style="list-style-type: none"><li>• Key names</li><li>• Text typed into a GUI element, such as into a box</li><li>• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes</li></ul>
<i>Italics font</i>	Text emphasis
Monospace font	<ul style="list-style-type: none"><li>• File and directory names</li><li>• System output</li><li>• Code</li><li>• Text typed at the command-line</li></ul>
<i>Monospace italic font</i>	<ul style="list-style-type: none"><li>• Code variables</li><li>• Command-line variables</li></ul>
<b>Monospace, bold font</b>	Emphasis of file and directory names, system output, code, and text typed at the command-line



**WARNING!** Indicates that failure to follow directions could result in bodily harm or death.



**CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.



**IMPORTANT:** Provides clarifying information or specific instructions.



**NOTE:** Provides additional information.



**TIP:** Provides helpful hints and shortcuts.

---

# HP technical support

Telephone numbers for worldwide technical support are listed on the following HP web site:  
<http://www.hp.com/support/>. From this web site, select the country of origin.



**NOTE:** For continuous quality improvement, calls may be recorded or monitored.

---

Obtain the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

## HP Storage web site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at:  
<http://www.hp.com/country/us/eng/prodserv/storage.html>. From this web site, select the appropriate product or solution.

## HP authorized reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518.
- Elsewhere, visit <http://www.hp.com> and click **Contact HP** to find locations and telephone numbers.



# 1 Introduction to system messages

This guide supports Fabric OS v4.4.0 and contains system messages useful for diagnosing and fixing problems with switches and fabrics. The messages are organized alphabetically by module name. A *module* is a subsystem in Fabric OS. Each module generates a set of numbered messages.

For each message, this guide provides message text, probable cause, recommended action, and severity level. Messages can have more than one cause and more than one corrective action. This guide provides the most probable cause and recommends the most useful corrective action.

This chapter provides an introduction to the system messages and contains the following sections:

- [Changes for this release of Fabric OS](#), page 23
- [Changes to this guide for OS v5.0.0](#), page 24
- [Message severity levels](#), page 29
- [Overview of the system messages](#), page 29
- [Viewing and configuring the system message logs](#), page 32
- [Reading a system message](#), page 34
- [Responding to a system message](#), page 37
- [System module descriptions](#), page 38

---

## Changes for this release of Fabric OS

The following are major changes to error messages for this release of Fabric OS:

- The titles of messages have changed. Previous versions of Fabric OS (v4.2 and earlier) used the module name followed by an alphabetical description as the message name; for example, BLADE-FAULT. The new names for messages use the module name followed by a numeric identifier; for example, BL-1003. All messages appear in order, but not all message numbers are used.
- The number of severity levels has changed. Previous versions of Fabric OS (v4.2 and earlier) had six levels of severity, Panic through Debug. The Panic and Critical levels have been merged; the Debug and Info levels have also been merged. As a result, many messages now have new severity levels. The current version of Fabric OS (v4.4.0) has the following four levels of severity:
  - 1 for Critical
  - 2 for Error
  - 3 for Warning
  - 4 for Info

For more information, see "[Message severity levels](#)" on page 29.

- A new security audit flag has been added so that messages reporting sensitive security changes are flagged as `AUDIT` in the error log and provide more detailed information about the security commands that have been run, the user who ran them, and whether the action was successful. For more information, see "[Security audit logging](#)" on page 30.

- The message format has changed. Previous versions of Fabric OS used the following format:

*severity, Module-alphaname, severity\_number, message\_text*

Error messages now use the following format:

*timestamp, [Module-Number], sequence-number, [AUDIT], severity, switch-chassis-name, message-text*

- All messages are saved in persistent storage in this release. Previous releases normally saved only Panic and Critical levels in persistent storage. All commands related to managing persistent storage are removed in this release.
- The sequence number of error messages within the error log has new behavior. Messages are numbered sequentially from 1 to 2,147,483,647 (0x7ffffff). The sequence number continues to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the `errClear` command. The sequence number is persistent across power cycles and switch reboots.

---

## Changes to this guide for OS v5.0.0

The following changes are new to v5.0.0 and are not included elsewhere in this guide.

### ZONE audit messages

This section contains updates to the *HP StorageWorks Fabric OS 5.0.0 diagnostic and systems error message reference guide*.

#### ZONE-3001

##### Message

```
<timestamp>, [ZONE-3001], <sequence-number>, AUDIT, INFO,
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event
Name>, Status: <Event Status>, Info: <Zone object type> \"<Zone object
member list>\" added to <Zone object set type> \"<Zone object set
name>\".
```

##### Probable cause

Indicates that a new zone object member or members have been added to a zone object set.

A zone object may be an alias, zone member, zone, or zone configuration. The string "..." appears at the end of the zone object member list if the list is truncated in the message.

##### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action, as defined by your enterprise security policy.

##### Severity

INFO



## ZONE-3002

### Message

```
<timestamp>, [ZONE-3002], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Zone object set type> \"<Zone  
object set name>\" created with <Zone object type> \"<Zone object  
member list>\".
```

### Probable cause

Indicates that a new zone object set was created with the specified zone object member or members added.

A zone object may be an alias, zone member, zone, or zone configuration. The string "..." appears at the end of the zone object member list if the list is truncated in the message.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action, as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3003

### Message

```
<timestamp>, [ZONE-3003], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Zone object type> \"<Zone object  
name>\" deleted.
```

### Probable cause

Indicates that a specified zone object has been deleted.

A zone object may be an alias, zone member, zone, or zone configuration.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3004

### Message

```
<timestamp>, [ZONE-3004], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Zone object type> \"<Zone object  
member list>\" removed from <Zone object set type> \"<Zone object set  
name>\".
```

### Probable cause

Indicates that a specified zone object member or members have been removed from a specified zone object set.

A zone object may be an alias, zone member, zone or zone configuration. The string "..." appears at the end of the zone object member list if the list is truncated in the message.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3005

### Message

```
<timestamp>, [ZONE-3005], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: All zone information cleared from  
transaction buffer.
```

### Probable cause

Indicates that all zone information has been cleared from the transaction buffer.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3006

### Message

```
<timestamp>, [ZONE-3006], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Current zone configuration  
disabled.
```

### Probable cause

Indicates that the current zone configuration has been disabled.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3007

### Message

```
<timestamp>, [ZONE-3007], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Zone configuration \"<Zone  
configuration>\" enabled.
```

### Probable cause

Indicates that a specified zone configuration has been enabled.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3008

### Message

```
<timestamp>, [ZONE-3008], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Current zone configuration saved  
to flash.
```

### Probable cause

Indicates that the current zone configuration has been saved to flash.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3009

### Message

```
<timestamp>, [ZONE-3009], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: <Event Description>
```

### Probable cause

Indicates that a zone transaction has been aborted.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3010

### Message

```
<timestamp>, [ZONE-3010], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Zone object \"<Zone object name>\"  
copied to new zone object \"<New Zone object name>\".
```

### Probable cause

Indicates that a specified zone object has been copied to a new zone object.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3011

### Message

```
<timestamp>, [ZONE-3011], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Zone object \"<Zone object name>\"  
expunged.
```

### Probable cause

Indicates that a specified zone object has been expunged.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## ZONE-3012

### Message

```
<timestamp>, [ZONE-3012], <sequence-number>, AUDIT, INFO,  
<system-name>, User: <User Name>, Role: <User Role>, Event: <Event  
Name>, Status: <Event Status>, Info: Zone object \"<Zone object name>\"  
renamed to \"<New Zone object name>\".
```

### Probable cause

Indicates that a specified zone object has been renamed.

### Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

---

## Message severity levels

The four levels of severity for messages are Critical, Error, Warning, and Info. In general, the definitions of these severity levels are broad and serve as general guidelines for troubleshooting. For all cases, you should consider each message description thoroughly before taking action. System messages have the severity levels explained in [Table 2](#).

**Table 2** Message severity levels

Level	Description
1 Critical	A critical-level message indicates that the software has detected a serious problem that is going to cause a partial or complete failure of a subsystem if not corrected immediately. For example, a power supply failure or rise in temperature must receive immediate attention.
2 Error	Error-level messages report error conditions that do not significantly affect overall system functionality. For example, error-level messages may indicate timeouts on specific operations, failures of operations after retries, invalid parameters, or failure to perform a requested operation.
3 Warning	Warning-level messages highlight current operating conditions that, if not checked, may lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode. The failed power supply should be replaced or repaired.
4 info	Info-level messages report the current non-error status of system components; for example, the detection of online and offline status of a fabric port.

---

## Overview of the system messages

This section provides information on the various logs saved by the system and provides instructions for viewing the information in the log files. The following topics are discussed:

- [System message log \(RASLog\)](#), page 30
- [Security audit logging](#), page 30
- [Dual-CP systems](#), page 31
- [System logging daemon](#), page 31
- [Port logs](#), page 31
- [Panic dump and core dump files](#), page 31
- [Trace dumps](#), page 32
- [The supportSave command](#), page 32

- [System console](#), page 32

## System message log (RASLog)

Fabric OS maintains an internal system message log of all messages. For Fabric OS v4.4.0, this log is saved as a RASLog. Features of the system message log include the following:

- The saving of all messages to nonvolatile storage.
- A maximum of 1024 messages that can be saved in RAM.
- Implementation as a circular buffer. When more than the maximum number of entries are added to the log file, old entries are overwritten by new ones.
- The display of all system messages from the `errDump` and `errShow` commands.

Configure the `syslogd` facility as a management tool for error logs. This is particularly important for dual-domain switches, because the `syslogd` facility saves messages from two control processors (CPs) as a single file and in sequential order. See "[System logging daemon](#)" on page 31 for more information.

## Security audit logging

Audit messages are enhanced to record more information for security purposes. They are flagged `AUDIT` in the system message log. Currently, the only messages that have the audit flag set are SEC-3001 through SEC-3017.

These messages provide the following information:

- User Name: the name of the user who triggered the action.
- Role: The role of the user; for example, `root` or `admin`.
- Event Name: The name of the event that occurred.
- Status: The status of the event that occurred as success or failure.
- Event Info: Information about the event. If you are creating an `SCC_POLICY` and use wild cards such as the asterisk (\*), which means all the switches in the current fabric, these wild cards are displayed in the audit error message.

The following is an example of an audit message:

```
2004/07/09-02:09:40, [SEC-3001], 181, AUDIT, INFO, User:rick, role: admin, Event:
secpolicy create, status:success, Info: Create SCC_POLICY policy, with * entries.
```

Only certain commands generate an `AUDIT` message in the system message log. The commands that generate `AUDIT` messages are:

- `secModeEnable` and `secModeDisable`
- `secPolicyCreate`, `secPolicyDelete`, `secPolicyRemove`, `secPolicyActivate`, and `secPolicySave`
- `login` and `logout`
- `secFCSFailover`
- `secTransAbort`
- `secStatsReset`
- `secTempPasswdSet` and `secTempPasswdReset`
- `aaaConfig`
- `authUtil`

## Dual-CP systems

For both the Core Switch 2/64 and the SAN Director 2/128, each CP has a unique error log, depending on which CP was is when a message is reported. To fully understand message logging on the Core Switch 2/64 or the SAN Director 2/128, you should enable the system logging daemon, because the logs on the host computer are maintained in a single merged file for both CPs and are in sequential order. Otherwise, you must examine the error logs in both CPs, particularly for events such as `firmwareDownload` or `haFailover`, for which the active CP changes.

For both the Core Switch 2/64 and the SAN Director 2/128, security violations such as telnet, HTTP, and serial connection violations are not propagated between CPs. Security violations on the active CP are not propagated to the standby CP counters in the event of a failover, nor do security violations on the standby CP get propagated to the active CP counters.

## System logging daemon

The system logging daemon (syslogd) is a process on UNIX®, Linux®, and some Windows® systems that reads and logs messages as specified by the system administrator.

Fabric OS can be configured to use a UNIX-style syslogd process to forward system events and error messages to log files on a remote host system.

The host system can be running UNIX, Linux, or any other operating system that supports the standard syslogd functionality.

Configuring for syslogd involves configuring the host, enabling syslogd on the HP StorageWorks model, and, optionally, setting the facility level.

For information on configuring syslogd functionality, refer to the *HP StorageWorks Fabric OS 4.x procedures user guide*.

## Port logs

Fabric OS maintains an internal log of all port activity. Each switch or logical switch maintains a log file for each port. Port logs are circular buffers that can save up to 8000 entries per logical switch. When the log is full, the newest log entries overwrite the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device A-to-device B, and control information. Port logs are not persistent and are lost over power cycles and reboots.

Use the `portLogShow` command to display the port logs for a particular port. Use the `portLogEventShow` command to display the specific events reported for each port. Refer to the *HP StorageWorks Fabric OS 4.x procedures user guide* for information on interpreting results of the `portLogDump` command.



**NOTE:** Port log functionality is completely separate from the system message log. Port logs are typically used to troubleshoot device connections.

---

## Panic dump and core dump files

Fabric OS creates panic dump files and core files when problems occur in the Fabric OS kernel. These files can build up in the kernel partition (typically because of failovers) and may need to be periodically deleted or downloaded using the `saveCore` command. In case of a panic dump, view the files by issuing the `pdShow` command.

The software watchdog process (SWD) is responsible for monitoring daemons critical to the function of a healthy switch. The SWD holds a list of critical daemons that ping the SWD periodically at a predetermined interval defined for each daemon.

If a daemon fails to ping the SWD within the defined interval, or if the daemon terminates unexpectedly, the SWD dumps information to the panic dump files, which helps to diagnose the root cause of the unexpected failure.

Use the `pdShow` command to view these files or the `saveCore` command to send them to a host workstation using FTP. The panic dump files and core files are intended for support personnel use only.

## Trace dumps

Fabric OS produces trace dumps when problems are encountered within Fabric OS modules. Initiate the sending of trace dump files to support personnel using the `supportSave` or `traceFtp` command. Fabric OS trace dump files are intended for use only by support personnel.

## The supportSave command

The `supportSave` command can be used to send by FTP the output of the system messages (RASLog), the trace files, and the output of the `supportShow` command to a support location. Before running the `supportSave` command, you can, as an option, set up the FTP parameters using the `supportFtp` command. The `supportShow` command runs a large number of dump and show commands to provide a global output of the status of the switch. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on these commands.

## System console

The system console displays messages only through the serial port. If you log in to a switch through the Ethernet port or modem port, you do not receive system console messages.

The `errFilterSet` command can be used by administrators to filter messages that appear on the system console by severity level. All messages are still sent to the system message log and to the syslog, if enabled.

The system console displays both system messages and panic dump messages. These messages are mirrored to the system console; they are always saved in one of the system logs.

---

# Viewing and configuring the system message logs

Use the commands in [Table 3](#) to view or configure the system message logs. Many of these commands require admin login privileges to execute.

**Table 3** Commands to view and configure system logs

Command	Description
<code>agtCfgDefault</code>	Resets the SNMP recipients to default values.
<code>agtCfgSet</code>	Configures the SNMP recipients.
<code>agtCfgShow</code>	Displays the current configuration of the SNMP recipients.
<code>errClear</code>	Clears the error log.
<code>errDelimiterSet</code>	Sets the error log start and end delimiter for messages pushed to the console.
<code>errDump</code>	Displays the entire error log without page breaks. Use the <code>-r</code> option to show the messages in reverse order, from newest to oldest.
<code>errFilterSet</code>	Sets an error severity filter for the system console.



**Table 3** Commands to view and configure system logs (continued)

Command	Description
<code>errShow</code>	Displays the entire error log with page breaks. Use the <code>-r</code> option to show the messages in reverse order, from newest to oldest.
<code>pdShow</code>	Displays the contents of the panic dump and core dump files.
<code>portErrShow</code>	Displays the port error summary.
<code>portLogClear</code>	Clears the port log. If the port log is disabled, this commands enables it.
<code>portLogDisable</code>	Disables the port log facility.
<code>portLogDump</code>	Displays the port log without page breaks.
<code>portLogDumpPort</code>	Displays the port log of the specified port without page breaks.
<code>portLogEventShow</code>	Displays which port log events are currently being reported.
<code>portLoginShow</code>	Displays port logins.
<code>portLogPdisc</code>	Sets or clear the debug <code>pdisc_flag</code> .
<code>portLogReset</code>	Enables the port log facility.
<code>portLogResize</code>	Resizes the port log to the specified number of entries.
<code>portLogShow</code>	Displays the port log with page breaks.
<code>portLogShowPort</code>	Displays the port log of a port with page breaks for a specific port.
<code>portLogTypeDisable</code>	Disables an event from reporting to the port log. Port log events are described by the <code>portLogEventShow</code> command.
<code>portLogTypeEnable</code>	Enables an event to report to the port log. Port log events are described by the <code>portLogEventShow</code> command.
<code>saveCore</code>	Saves or removes core files created by the kernel.
<code>setVerbose</code>	Sets the verbose level of a particular module within Fabric OS.
<code>supportFtp</code>	Sets, clears, or displays support FTP parameters or a time interval to check the FTP server.
<code>supportSave</code>	Collects RASLog, trace files, and <code>supportShow</code> (active CP only) information for the local CP and then transfers the files to an FTP server. The operation can take several minutes.
<code>supportShow</code>	Executes a list of diagnostic and error display commands. The output is used by your switch service provider to diagnose and correct problems with the switch. The output from this command is very long.
<code>syslogDIpAdd</code>	Adds an IP address as a recipient of system messages.
<code>syslogDIpRemove</code>	Removes an IP address as a recipient of system messages.

**Table 3** Commands to view and configure system logs (continued)

Command	Description
syslogDIpShow	Displays the currently configured IP addresses that are recipients of system messages.
syslogdFacility	Changes the syslogd facility.
traceDump	Displays, initiates, or removes a Fabric OS module trace dump.
traceFtp	Displays, enables, or disables the trace auto-FTP or retrieves the trace dump file.
traceTrig	Sets, removes, or displays trace triggers.

## Reading a system message

This section provides information about reading system messages.

### Example system message

The following example shows a sample message from the error log:

```
2004/07/22-10:12:33, [EM-1031], 4,, ERROR, switchname, Slot 7 ejector not closed
```

The fields in the error message are described in [Table 4](#).

**Table 4** Error message field description

Example	Variable name	Description
2004/07/22-10:12:33	Date and Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an internationalized timestamp format base on the LOCAL setting.
[EM-1031]	Message Module and Message Number	Displays the message module and number. These values uniquely identify each message in Fabric OS and reference the cause and actions in this manual.

**Table 4** Error message field description (continued)

Example	Variable name	Description
4	Sequence Number	<p>The error message position in the log. When any messages are added to the log, this number is incremented. When this message reaches the last position in the error log and becomes the oldest message, it is deleted when a new message is added.</p> <p>In Fabric OS v4.4.0, the message sequence number starts at 1 after a <code>firmwareDownload</code> and increases up to a value of 2,147,483,647 (0x7fffffff).</p> <p>The sequence number continues to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the <code>errClear</code> command. The sequence number is persistent across power cycles and switch reboots.</p>
, <AUDIT>, (not shown in the previous example)	Audit Flag	Indicates that this message is an AUDIT message for a security issue. The only messages that have the audit flag set are SEC-3001 through SEC-3017. For all other messages, this field is blank. The commas still appear, so many messages have two commas separated by a blank space.
<i>SEVERITY</i>	Severity Level	Displays the severity of the error as Critical, Error, Warning, or Info
<i>switchname</i>	Switch name or chassis name, depending on the action. For example, HA messages typically show the chassis name; login failures typically show the logical switch name.	Displays the defined switch name or the chassis name of the switch. The value is truncated if it is more than 16 characters. Use either the <code>chassisName</code> command to name the chassis or the <code>switchName</code> command to rename the logical switch.
Slot 7 ejector not closed	Error Description	Displays a text string explaining the error encountered and providing parameters supplied by the software at runtime.

## Viewing system messages from Advanced Web Tools

This procedure is valid for the HP StorageWorks SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/16N, SAN Switch 2/32, SAN Switch 4/32, Core Switch 2/64, and SAN Director 2/128.

To view the system message log for a switch from Advanced Web Tools:

1. Launch Advanced Web Tools.
2. Select the desired switch from the Fabric Tree.

The Switch View displays.

3. Click the **Switch Events** button.

A Switch Events Report opens.

4. View the switch events and messages.

In dual-domain switches, an Event button exists for each logical switch. Only messages relating to that switch (and chassis) are displayed.

## Dumping the system messages

This procedure is valid for the HP StorageWorks SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/16N, SAN Switch 2/32, SAN Switch 4/32, Core Switch 2/64, and SAN Director 2/128.

To display the system message log with no page breaks:

1. Log in to the switch as the admin user.
2. Issue the `errDump` command:

```
switch:admin> errDump
Version: 4.4.0
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in sync

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out of
sync

2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port
media incompatible. Reason: Configured port speed.

2004/07/28-17:04:54, [FABR-1001], 4,, WARNING, switch, port 4, ELP
rejected by the other switch

2004/07/28-17:05:06, [FW-1050], 5,, WARNING, switch, Sfp Supply Voltage
0, is below low boundary(High=3600, Low=3150). Current value is 0 mV.

switch:admin>
```

## Viewing the system messages with page breaks

This procedure is valid for the HP StorageWorks SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/16N, SAN Switch 2/32, SAN Switch 4/32, Core Switch 2/64, and SAN Director 2/128.

To display the system message log with page breaks:

1. Log in to the switch as the admin user.

## 2. Issue the `errShow` command:

```
switch:admin> errShow
Version: 4.4.0
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in sync

Type <CR> to continue, Q<CR> to stop:

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out of
sync

Type <CR> to continue, Q<CR> to stop:

2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port
media incompatible
e. Reason: Configured port speed.

Type <CR> to continue, Q<CR> to stop:
```

## Clearing the system message log

This procedure is valid for the HP StorageWorks SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/16N, SAN Switch 2/32, SAN Switch 4/32, Core Switch 2/64, and SAN Director 2/128.

To clear the system message log for a particular switch instance:

1. Log in to the switch as the admin user.
2. Issue the `errClear` command to clear all messages from memory.

The following example shows how to clear the system message log:

```
switch:admin> errclear
switch:admin>
```

---

## Responding to a system message

This section provides procedures on gathering information about system messages.

### Looking up a system message

Error messages are arranged in this guide alphabetically. To look up an error message, copy down the message module (see [Table 4](#) on page 34) and the message number and compare these with the Table of Contents to determine the location of the information for that error message. [Table 5](#) describes each of the message modules.

## Gathering information about the problem

Steps to take when troubleshooting include the following:

1. Determine the current Fabric OS level.
2. Determine the switch hardware version.
3. Determine whether the switch is operational.
4. Assess impact and urgency:
  - Is the switch down?
  - Is it a standalone switch?

- How large is the fabric?
  - Is the fabric redundant?
5. Issue the `errDump` command on each logical switch.
  6. Issue the `supportFtp` command as needed to set up automatic FTP transfers and then issue the `supportSave` command.
  7. Document the sequence of events by answering the following questions:
    - What happened just prior to the problem?
    - Is the problem repeatable?
    - If so, what are the steps to produce the problem?
    - What configuration was in place when the problem occurred?
  8. Determine whether a failover occurred.
  9. Determine whether security was enabled.
  10. Determine whether power-on self test (POST) was enabled.
  11. Determine whether serial port (console) logs are available.
  12. Determine which CP was master (applicable only to the Core Switch 2/64 or SAN Director 2/128).
  13. Identify the last actions or changes made to the system.

## System module descriptions

Table 5 provides a summary of the system modules for which messages are documented in this reference guide in “Messages” on page 47; the system modules are listed alphabetically by name.

**Table 5** System module descriptions

System module	Description
AUTH	Authentication error messages indicate problems with the authentication module of Fabric OS.
BL	Blade error messages are a result of faulty hardware, transient out-of-memory conditions, ASIC errors, or inconsistencies in the software state between a blade and the environment monitor (EM) module.
BLL	Bloom is the name of the ASIC used as the building block for third-generation hardware platforms.
CER	The core edge routing module on the SAN Director 2/128 platform.

**Table 5** System module descriptions (continued)

System module	Description
EM	<p>The EM manages and monitors the various field replaceable units (FRUs), including the port cards, CP blades, blower assemblies, power supplies, and World Wide Name (WWN) cards. EM controls the state of the FRUs during system startup, hot-plug sequences, and fault recovery.</p> <p>EM provides access to and monitors the sensor and status data from the FRUs and maintains the integrity of the system using the environmental and power policies. EM reflects system status through telnet commands, system LEDs, and status and alarm messages. EM also manages some component-related data.</p>
EVMD	Event management module.
FABR	A fabric is a network of Fibre Channel switches. The FABR error messages come from the fabric daemon. The fabric daemon follows the FC-SW-3 standard for the fabric initialization process, such as determining the E_Ports, assigning unique domain IDs to switches, creating a spanning tree, throttling the trunking process, and distributing the domain and alias lists to all switches in the fabric.
FABS	Fabric OS system driver module.
FCMC	Fibre Channel miscellaneous messages relate to problems with the physical layer used to send Fibre Channel traffic to and from the switch.
FCPD	The Fibre Channel Protocol daemon is responsible for probing the devices attached to the loop port. Probing is a process the switch uses to find the devices attached to the loop ports and to update the Name Server with the information.
FCPH	Fibre Channel Physical Layer is used to send Fibre Channel traffic to and from the switch.
FKLB	Fabric OS I/O kernel library module.
FLOD	A part of the Fabric Shortest Path First (FSPF) protocol that handles synchronization of the Link State Database (LSDB) and propagation of the Link State Records (LSRs).
FSPF	Fabric shortest path first is a link state routing protocol that determines how frames should be routed. These messages are about protocol errors.

**Table 5** System module descriptions (continued)

System module	Description
FSS	<p>The Fabric OS state synchronization framework provides facilities by which the active CP can synchronize with the standby CP, enabling the standby CP to take control of the switch non-disruptively during failures and software upgrades. These facilities include version negotiation, state information transfer, and internal synchronization functions, enabling the transition from standby to active operation.</p> <p>FSS is defined both as a component and a service. A <i>component</i> is a module in Fabric OS, implementing a related set of functionality. A <i>service</i> is a collection of components grouped together to achieve a modular software architecture.</p>
FSSM	<p>The Fabric OS state synchronization management module is defined both as a component and a service. A component is a module in Fabric OS implementing a related set of functionality. A service is a collection of components grouped together to achieve a modular software architecture.</p>
FW	<p>The Fabric Watch module monitors thresholds for many switch subsystems: for example, temperature, voltage, fan speed, and switch status. Any changes that cross a specified threshold are reported to the system message log.</p>
HAM	<p>A user space daemon responsible for high-availability management.</p>
HAMK	<p>The kernel module for the HAM daemon.</p>
HIL	<p>Hardware Independent Layer.</p>
HLO	<p>Part of FSPF protocol that handles the HELLO protocol between adjacent switches. The HELLO protocol establishes connectivity with a neighbor switch to determine the identity of the neighbor switch and to exchange FSPF parameters and capabilities.</p>
HMON	<p>Health monitor.</p>
HTTP	<p>HTTP error message.</p>



**Table 5** System module descriptions (continued)

System module	Description
KSWD	<p>The Kernel Software Watchdog monitors daemons for unexpected terminations and hang conditions; KSWD informs the HAM module to take corrective actions, such as failover or reboot.</p> <p>The following daemons are monitored by KSWD:</p> <ul style="list-style-type: none"> <li>• Diagnostics daemon (DIAGD)</li> <li>• Environment Monitor daemon (EMD)</li> <li>• EVM daemon (EVMD)</li> <li>• Fabric daemon (FABRICD)</li> <li>• FCPD daemon (FCPD)</li> <li>• FDMI daemon (FDMID)</li> <li>• FSPF daemon (FSPFD)</li> <li>• Fabric Watch daemon (FWD)</li> <li>• Management Server daemon (MSD)</li> <li>• Name Server daemon (NSD)</li> <li>• PDM daemon (PDMD)</li> <li>• PS daemon (PSD)</li> <li>• Reliable Commit Service daemon (RCSD)</li> <li>• FA-API RPC daemon (RPCD)</li> <li>• Security daemon (SECD)</li> <li>• SNMP daemon (SNMPD)</li> <li>• Track Changes daemon (TRACK_CHANGES)</li> <li>• Time Service daemon (TSD)</li> <li>• Web Tools daemon (WEBD)</li> <li>• Zone daemon (ZONED)</li> </ul>
KTRC	Kernel RAS trace module.
LOG	RASLog subsystem.
LSDB	The link state database is a part of the FSPF protocol that maintains records on the status of port links. This database is used to route frames.
MPTH	Multicast path uses the Shortest Path First (SPF) algorithm to dynamically compute a broadcast tree.

**Table 5** System module descriptions (continued)

System module	Description
MQ	Message queues are used for interprocess communication. Message queues allow many messages, each of variable length, to be queued. Any process or Interrupt Service Routine (ISR) can write messages to a message queue. Any process can read messages from a message queue.
MS	<p>The Management Service enables the user to obtain information about the Fibre Channel fabric topology and attributes by providing a single management access point. MS provides for both monitoring and control of the following areas:</p> <ul style="list-style-type: none"> <li>• Fabric Configuration Server, which provides for the configuration management of the fabric.</li> <li>• Unzoned Name Server, which provides access to Name Server information that is not subject to zone constraints.</li> <li>• Fabric Zone Server, which provides access to and control of zone information.</li> </ul>
NBFS	<p>NBFSM is a part of the FSPF protocol that handles a neighboring or adjacent switch's Finite State Machine (FSM).</p> <p>Input to the FSM changes the local switch from one state to another, based on specific events. For example, when two switches are connected to each other using an interswitch link (ISL) cable, they are in the Init state. After both switches receive HELLO messages, they move to the Database Exchange state, and so on.</p> <p>NBFSM states are Down (0), Init (1), Database Exchange (2), Database Acknowledge Wait (3), Database Wait (4), and Full (5).</p>
NS	Indicates problems with the Simple Name Server module.
PDM	Parity data manager is a user space daemon responsible for the replication of persistent configuration files from the primary partition to the secondary partition and from the active CP blade to the standby CP blade.
PDTR	These messages indicate that panic dump trace files have been created.
PORT	PORT error messages refer to the front-end user ports on the switch. Front-end user ports are directly accessible by users to connect end devices or to connect to other switches.

**Table 5** System module descriptions (continued)

System module	Description
PLAT	Platform (Service) errors are generated from the port blade and CP blade of the Core Switch 2/64, the SAN Director 2/128, and the ASICs or motherboard components of all other switches. These error messages usually indicate hardware problems in these components, including problems resulting from the PCI buses, i2c bus, field-programmable gate array (FPGA), and power supply.
PS	The performance server daemon measures the amount of traffic between end points or traffic with particular frame formats, such as SCSI frames, IP frames, and customer-defined frames.
PSWP	The portswap feature and associated commands generate these error messages.
RCS	The Reliable Commit Service daemon generates log entries when it receives a request from the zoning, security, or management server for passing data messages to switches in the fabric. RCS then requests Reliable Transport Write and Read (RTWR) to deliver the message. RCS also acts as a gatekeeper, limiting the number of outstanding requests for the Zoning, Security, or Management Server modules.
RPCD	The Remote Procedure Call Daemon (RPCD) is used by Fabric Access for API-related tasks.
RTWR	The Reliable Transport Write and Read daemon helps deliver data messages either to specific switches in the fabric or to all of the switches in the fabric. For example, if some of the switches are not reachable or are offline, RTWR returns an <code>unreachable</code> message to the caller, allowing the caller to take the appropriate action. If a switch is not responding, RTWR retries 100 times.
SCN	The internal state change notification daemon is used for state change notifications from the kernel to the daemons within Fabric OS.
SEC	The security daemon generates security errors, warnings, or information during security-related data management or fabric merge operations. Administrators should watch for these messages, to distinguish between internal switch and fabric operation errors, and external attack.
SNMP	Simple Network Management Protocol is a universally supported low-level protocol that allows simple get, get next, and set requests to go to the switch (acting as an SNMP agent). It also allows the switch to send traps to the defined and configured management station. HP StorageWorks switches support six management entities that can be configured to receive these traps.

**Table 5** System module descriptions (continued)

System module	Description
SS	The <code>supportSave</code> command generates these error messages if problems are encountered.
SULB	The software upgrade library provides <code>firmwareDownload</code> command capability, which enables firmware upgrades to both CP blades with a single command, as well as nondestructive code load to all 4.x switches. These messages display if problems occur during the <code>firmwareDownload</code> procedure. Most messages are informational only and are generated even during successful firmware download. For additional information, refer to the <i>HP StorageWorks Fabric OS 4.x procedures user guide</i> .
SWCH	These messages are generated by the switch driver module that manages a Fibre Channel switch instance.
SYSC	System controller is a daemon that starts up and shuts down all Fabric OS modules in the proper sequence.
SYSM	General system messages.
TRCE	RAS TRACE error messages.
TRCK	<p>The track change feature tracks the following events:</p> <ul style="list-style-type: none"> <li>• Turning on or off the track change feature</li> <li>• CONFIG_CHANGE</li> <li>• LOGIN</li> <li>• LOGOUT</li> <li>• FAILED_LOGIN</li> </ul> <p>If any of these events occurs, a message is sent to the system message log. If the SNMP trap option is enabled, an SNMP trap is also sent.</p> <p>For information on configuring the track change feature, refer to the <i>HP StorageWorks Fabric OS 4.x command reference guide</i> or the <i>HP StorageWorks Fabric OS 4.x procedures user guide</i>.</p>
TS	Time Service provides fabric time-synchronization by synchronizing all clocks in the fabric to the clock time on the principal switch.
UCST	UCAST is a part of the FSPF protocol that manages the Unicast routing table.
UPTH	UPATH is a part of the FSPF protocol that uses the SPF algorithm to dynamically compute a Unicast tree.

**Table 5** System module descriptions (continued)

System module	Description
USWD	The User-space Software Watchdog Daemon informs the KSWD about which daemons the watchdog subsystem monitors. The USWD daemon also helps the KSWD daemon to print debug information if a critical daemon has an unexpected termination.
WEBD	Indicates problems with the Web Tools module.
ZOLB	Indicates problems with the zone library module.
ZONE	The zone module messages indicate any problems associated with the zoning features, including commands associated with aliases, zones, and configurations.



## 2 Messages

### Authentication error messages

#### AUTH-1001

##### Message

```
timestamp, [AUTH-1001], sequence-number,, INFO, system-name,  
Operation-type has been successfully done.
```

##### Probable cause

The secret database operation has been updated using the `secAuthSecret` command. The values for `Operation-type` are `set` and `remove`.

##### Recommended action

No action is required.

##### Severity

INFO

#### AUTH-1002

##### Message

```
timestamp, [AUTH-1002], sequence-number,, ERROR, system-name,  
Operation-type has failed.
```

##### Probable cause

The specified action failed to update the secret database using the `secAuthSecret` command. The values for `Operation-type` are `set` and `remove`.

##### Recommended action

1. Retry the `secAuthSecret` command.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

##### Severity

ERROR

# AUTH-1003

## Message

```
timestamp, [AUTH-1003], sequence-number,, INFO, system-name, data-type  
type has been successfully set to setting value.
```

## Probable cause

An authentication configuration value was set to a specified value. The data type is either authentication type or DH group type.

## Recommended action

No action is required.

## Severity

INFO

# AUTH-1004

## Message

```
timestamp, [AUTH-1004], sequence-number,, ERROR, system-name, Failed to  
set data type type to setting-value.
```

## Probable cause

The `authUtil` command failed to set the authentication configuration value. The data type can be either authentication type or DH group type.

## Recommended action

1. Retry the `authUtil` command.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1005

## Message

```
timestamp, [AUTH-1005], sequence-number,, ERROR, system-name,  
Authentication file does not exist: error-code.
```

## Probable cause

Authentication file corruption.



## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1006

## Message

```
timestamp, [AUTH-1006], sequence-number,, WARNING, system-name, Failed to  
open authentication configuration-file.
```

## Probable cause

An internal problem with the Secure Fabric OS.

## Recommended action

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# AUTH-1007

## Message

```
timestamp, [AUTH-1007], sequence-number,, ERROR, system-name, The proposed  
authentication protocol(s) are not supported: port port-number.
```

## Probable cause

The proposed authentication protocol type or types are not supported by the local port.

## Recommended action

Run the `authUtil` command to make sure the local switch supports the specified protocols: FCAP or DH-CHAP.

## Severity

ERROR

# AUTH-1008

## Message

```
timestamp, [AUTH-1008], sequence-number,, ERROR, system-name, No security license, operation failed.
```

## Probable cause

The switch does not have a security license.

## Recommended action

Verify that the security license is installed using the `licenseShow` command. If necessary, reinstall the license using the `licenseAdd` command.

## Severity

ERROR

# AUTH-1010

## Message

```
timestamp, [AUTH-1010], sequence-number,, ERROR, system-name, Failed to initialize security policy: switch switch-number, error error-code.
```

## Probable cause

An internal problem with the Secure Fabric OS.

## Recommended action

1. Reboot or power cycle the switch.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1011

## Message

```
timestamp, [AUTH-1011], sequence-number,, WARNING, system-name, Failed to register for failover operation: switch switch-number error error-code
```

## Probable cause

An internal problem with the Secure Fabric OS.

## Recommended action

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# AUTH-1012

## Message

```
timestamp, [AUTH-1012], sequence-number,, WARNING, system-name,  
Authentication code is rejected: port port-number explain explain-code  
reason reason-code
```

## Probable cause

An authentication is rejected because the remote entity does not support authentication.

## Recommended action

Make sure the entity at the other end of the link supports authentication.

## Severity

WARNING

# AUTH-1013

## Message

```
timestamp, [AUTH-1013], sequence-number,, WARNING, system-name, Can not  
perform authentication request message: port port-number, message code  
message-code
```

## Probable cause

The system is running low on resources when receiving an authentication request.

## Recommended action

Usually this problem is transient. The authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# AUTH-1014

## Message

```
timestamp, [AUTH-1014], sequence-number,, ERROR, system-name, Invalid port  
value to operation: port port-number
```

## Probable cause

Internal problem with the Secure Fabric OS.

## Recommended action

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1017

## Message

```
timestamp, [AUTH-1017], sequence-number,, ERROR, system-name, Invalid  
value to start authentication request: port port-number, opcode  
operation-code
```

## Probable cause

Internal problem with the Secure Fabric OS.

## Recommended action

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1018

## Message

```
timestamp, [AUTH-1018], sequence-number,, ERROR, system-name, Invalid  
value to check protocol type: port port-number
```

## Probable cause

Internal problem with the Secure Fabric OS.

## Recommended action

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1020

## Message

```
timestamp, [AUTH-1020], sequence-number,, INFO, system-name, Failed to  
create timer for authentication: port port-number
```

## Probable cause

An authentication message's timer was not created.

## Recommended action

This problem is usually transient, although the authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

INFO

# AUTH-1022

## Message

```
timestamp, [AUTH-1022], sequence-number,, ERROR, system-name, Failed to  
extract data-type from message payload: port port-number.
```

## Probable cause

The authentication process failed to extract a particular value from the receiving payload.

## Recommended action

This problem is usually transient, although the authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1023

## Message

```
timestamp, [AUTH-1023], sequence-number,, ERROR, system-name, Failed to  
operation-type during authentication-phase: port port-number.
```

## Probable cause

An authentication operation failed for a certain authentication phase.

*Operation-type* varies depending on authentication type:

- Some operations for SLAP are certificate retrieve, certificate verification signature verification, and nonce signing.
- Some operations for FCAP are certificate retrieve, certificate verification, signature verification, and nonce signing.
- Some operations for DH-CHAP are response calculation, challenge generation, and secret retrieve.

The *authentication-phase* specifies the phase of a particular authentication protocol that failed.

A *nonce* is a single-use, usually random value used in authentication protocols to prevent replay attacks.

## Recommended action

1. The error may indicate that an invalid entity tried to connect to the switch. Check the connection port for possible unauthorized access attack.
2. It may indicate that the PKI object for SLAP or FCAP or the secret value for DH-CHAP on the local entity is not set up properly. Reinstall all PKI objects or reset the secret value for DH-CHAP properly.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.

4. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1025

## Message

```
timestamp, [AUTH-1025], sequence-number,, ERROR, system-name, Failed to  
get data-type during authentication-phase: port port-number
```

## Probable cause

The authentication process failed to get expected information during the specified authentication phase.

## Recommended action

This problem is usually transient, although the authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1027

## Message

```
timestamp, [AUTH-1027], sequence-number,, ERROR, system-name, Failed to  
select authentication-value during authentication-phase: value value port  
port-number.
```

## Probable cause

The authentication process failed to select an authentication value (that is, DH Group, hash value, or protocol type) from a receiving payload for a particular authentication phase. This indicates that the local switch does not support the specified authentication value.

## Recommended action

1. Check the authentication configuration and reset the supported value if needed using the `authUtil` command.
2. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1028

## Message

```
timestamp, [AUTH-1028], sequence-number,, ERROR, system-name, Failed to  
allocate data-type for operation-phase: port port-number
```

## Probable cause

The authentication process failed because the system is low on memory.

*Data-type* is the payload or structure that failed to get memory.

*Operation-phase* specifies which operation of a particular authentication phase failed.

## Recommended action

This problem is usually transient, although the authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1029

## Message

```
timestamp, [AUTH-1029], sequence-number,, ERROR, system-name, Failed to  
get data-type for message-phase message: port port-number, retval  
error-code
```

## Probable cause

The authentication process failed to get a particular authentication value at certain phase.

*Data-type* is the payload or structure that failed to get memory.

## Recommended action

This problem is usually transient, although the authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.



## Severity

ERROR

# AUTH-1030

## Message

```
timestamp, [AUTH-1030], sequence-number,, ERROR, system-name, Invalid  
message code for message-phase message: port port-number
```

## Probable cause

The receiving payload does not have a valid message code for a particular authentication phase.

## Recommended action

This problem is usually transient, although the authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1031

## Message

```
timestamp, [AUTH-1031], sequence-number,, ERROR, system-name, Failed to  
retrieve secret value: port port-number
```

## Probable cause

The secret value was not set properly for the authenticated entity.

## Recommended action

1. Reset the secret value by using `secAuthSecret` command.
2. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

## Severity

ERROR

# AUTH-1032

## Message

```
timestamp, [AUTH-1032], sequence-number,, ERROR, system-name, Failed to  
generate data-type for message-payload payload: length data-length, error  
code error-code, port port-number
```

## Probable cause

The authentication process failed to generate a particular data (that is, challenge, nonce, or response data) for an authentication payload. This usually relates to internal failure. A *nonce* is a single-use, usually random value used in authentication protocols to prevent replay attacks.

## Recommended action

This problem is usually transient, although the authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1033

## Message

```
timestamp, [AUTH-1033], sequence-number,, ERROR, system-name, Disable port  
port-number due to unauthorized switch switch-wwn-value
```

## Probable cause

An entity was not configured in the SCC policy and tried to connect to the port.

## Recommended action

Add the entity's WWN to the SCC policy and reinitialize authentication by using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

## Severity

ERROR

# AUTH-1034

## Message

```
timestamp, [AUTH-1034], sequence-number,, ERROR, system-name, Failed to  
validate name entity-name in authentication-message: port port-number
```

## Probable cause

The entity name in the payload is not in the right format.

## Recommended action

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1035

## Message

```
timestamp, [AUTH-1035], sequence-number,, ERROR, system-name, Invalid  
data-type length in message-phase message: length data-length, port  
port-number
```

## Probable cause

A data field in the authentication message has an invalid length field. This error usually indicates internal failure.

## Recommended action

This problem is usually transient, although the authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1036

## Message

```
timestamp, [AUTH-1036], sequence-number,, ERROR, system-name, Invalid  
state state-value for authentication-phase: port port-number
```

## Probable cause

The switch received an unexpected authentication message.

## Recommended action

This problem is usually transient, although the authentication may fail.

1. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers,
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1037

## Message

```
timestamp, [AUTH-1037], sequence-number,, ERROR, system-name, Failed to  
operation-type response for authentication-message: init_len data-length,  
resp_len data-length, port port-number.
```

## Probable cause

A DH-CHAP authentication operation failed on the specified port due to mismatched response values between two entities.

## Recommended action

1. The error may indicate that an invalid entity tried to connect to the switch. Check the connection port for a possible security attack.
2. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# AUTH-1038

## Message

```
timestamp, [AUTH-1038], sequence-number,, ERROR, system-name, Failed to  
retrieve certificate during authentication-phase: port port-number
```

## Probable cause

The PKI certificate is not installed properly.

## Recommended action

1. Reinstall the PKI certificate using the `pkiCreate` command.
2. Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

---

# Blade error messages

## BL-1000

## Message

```
timestamp, [BL-1000], sequence-number,, INFO, system-name, Initializing  
Ports...
```

## Probable cause

The switch has started initializing the ports. This message occurs only on the HP StorageWorks SAN Switch 4/32.

## Recommended action

No action is required.

## Severity

INFO

# BL-1001

## Message

```
timestamp, [BL-1001], sequence-number,, INFO, system-name, Port  
Initialization Completed
```

## Probable cause

The switch has completed initializing the ports. This message occurs only on the SAN Switch 4/32.

## Recommended action

No action is required.

## Severity

INFO

# BL-1002

## Message

```
timestamp, [BL-1002], sequence-number,, CRITICAL, system-name, Init  
Failed: DISABLED because internal ports were not ONLINE, Slot: slot-number
```

## Probable cause

The blade initiation failed because one or more of the internal ports was not online. The blade is faulted. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

1. Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.
2. Run the `systemVerification` command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
3. Additional blade fault messages precede and follow this error, providing more information. See other error messages for recommended action.
4. If the message persists, replace the blade.

## Severity

CRITICAL

# BL-1003

## Message

```
timestamp, [BL-1003], sequence-number,, CRITICAL, system-name, Faulting  
blade in slot slot-number
```

## Probable cause

A faulty blade in the specified slot number. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

1. Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.
2. Run the `systemVerification` command to verify that blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
3. If the message persists, replace the blade.

## Severity

CRITICAL

# BL-1004

## Message

```
timestamp, [BL-1004], sequence-number,, CRITICAL, system-name, Suppressing  
blade fault in slot slot-number
```

## Probable cause

The specified blade experienced a failure, but was not faulted due to a user setting. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

1. Reboot or power cycle the blade, using the `slotPowerOff` and `slotPowerOn` commands.
2. Run the `systemVerification` command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
3. If the message persists, replace the blade.

## Severity

CRITICAL

## BL-1006

### Message

```
timestamp, [BL-1006], sequence-number,, INFO, system-name, Blade  
slot-number NOT faulted. Peer blade slot-number experienced abrupt  
failure.
```

### Probable cause

The errors (mostly synchronization errors) on this blade are harmless. Probably, the standby CP blade connected to the active CP blade has experienced transitory problems. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

### Recommended action

Check the standby CP. No action is required if the other blade is already removed or faulted.

### Severity

INFO

## BL-1007

### Message

```
timestamp, [BL-1007], sequence-number,, WARNING, system-name, blade  
#blade-number: blade state is inconsistent with EM. bl_cflags  
0xblade-control-flags, slot_on slot-on-flag, slot_off slot-off-flag,  
faulty faulty-flag, status blade-status
```

### Probable cause

A failover occurred while a blade was initializing on the previously active CP. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

### Recommended action

No action is required. The blade is reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you may have to stop and restart the traffic during this process.

### Severity

WARNING



# BL-1008

## Message

```
timestamp, [BL-1008], sequence-number,, CRITICAL, system-name, Slot  
slot-number control-plane failure. Expected value: 0xvalue-1, Actual:  
0xvalue-2
```

## Probable cause

Possibly the blade has experienced a hardware failure or was removed without following the recommended removal procedure. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

1. Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.
2. Run the `systemVerification` command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
3. If the message persists, replace the blade.

## Severity

CRITICAL

# BL-1009

## Message

```
timestamp, [BL-1009], sequence-number,, CRITICAL, system-name, Blade in  
slot slot-number timed out initializing the chips.
```

## Probable cause

The blade has failed to initialize the ASIC chips. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

1. Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.
2. Run the `systemVerification` command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
3. If the message persists, replace the blade.

## Severity

CRITICAL

## BL-1010

### Message

```
timestamp, [BL-1010], sequence-number,, WARNING, system-name, Blade in  
slot slot-number inconsistent with the hardware settings.
```

### Probable cause

A failover occurred while some hardware changes were being made on the previously active CP (such as changing the domain ID). This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

### Recommended action

No action is required. This blade has been reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you may have to stop and restart the traffic during this process.

### Severity

WARNING

## BL-1011

### Message

```
timestamp, [BL-1011], sequence-number,, CRITICAL, system-name, Busy with  
emb-port int. for chip chip-number in minis minis-number on blade  
slot-number, chip int. is disabled. interrupt status=0xinterrupt-status
```

### Probable cause

Too many interrupts in the embedded port caused the specified chip to be disabled. The probable cause is too many abnormal frames; the chip is disabled to prevent the CP from becoming too busy.

### Recommended action

Capture the console output during the following process:

1. Check for a faulty cable, SFP, or device attached to the specified port.
2. Run the *systemVerification* command to verify that the blade or switch does not have hardware problems.
3. On a bladed switch, run the *slotPowerOff* and *slotPowerOn* commands.
4. On a non-bladed switch, reboot or power cycle the switch.
5. If the message persists, replace the blade.

### Severity

CRITICAL

# BL-1012

## Message

```
timestamp, [BL-1012], sequence-number,, INFO, system-name, bport  
port-number port int. is disabled. status=0xinterrupt-status Port  
port-number will be re-enabled in 1 minute.
```

## Probable cause

The port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The *port-number* is the blade port; this number may not correspond to a user port number.

## Recommended action

Capture the console output during the following process:

1. Check for a faulty cable, SFP, or device attached to the specified port.
2. On a bladed switch, run the `slotPowerOff` and `slotPowerOn` commands.
3. On a non-bladed switch, reboot or power cycle the switch.
4. If the message persists, replace the blade.

## Severity

INFO

# BL-1013

## Message

```
timestamp, [BL-1013], sequence-number,, INFO, system-name, bport  
port-number port is faulted. status=0xinterrupt-status Port port-number  
will be re-enabled in 1 minute.
```

## Probable cause

The port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The *port-number* is the blade port; this number may not correspond to a user port number.

## Recommended action

Capture the console output during the following process:

1. Check for a faulty cable, SFP, or device attached to the specified port.
2. On a bladed switch, run the `slotPowerOff` and `slotPowerOn` commands.
3. On a non-bladed switch, reboot or power cycle the switch.
4. If the message persists, replace the blade.

## Severity

INFO

# BL-1014

## Message

```
timestamp, [BL-1014], sequence-number,, INFO, system-name, bport  
port-number port int. is disabled. status=0xinterrupt-status
```

## Probable cause

The port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The *port-number* is the blade port; this number may not correspond to a user port number.

## Recommended action

Capture the console output during the following process:

1. On a bladed switch, run the `slotPowerOff` and `slotPowerOn` commands.
2. On a non-bladed switch, reboot the switch.
3. Run the `systemVerification` command to determine whether a hardware error exists.
4. If a hardware error does exist, or if the `slotPowerOff` or `slotPowerOn` fails on the bladed switch, or if errors are encountered again:
  - On the Core Switch 2/64 or SAN Director 2/128, replace the blade FRU.
  - On the SAN Switch 2/32, replace the motherboard FRU.
  - On the HP StorageWorks SAN Switch 2/8V, SAN Switch 2/16V, or SAN Switch 2/16N, SAN Switch 4/32, replace the switch.

## Severity

INFO

# BL-1015

## Message

```
timestamp, [BL-1015], sequence-number,, INFO, system-name, bport  
port-number port is faulted. status=0xinterrupt-status
```

## Probable cause

The port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The *port-number* is the blade port; this number may not correspond to a user port number.

## Recommended action

Capture the console output during the following process:

1. On a bladed switch, run the `slotPowerOff` and `slotPowerOn` commands.
2. On a non-bladed switch, reboot the switch.
3. Run the `systemVerification` command to determine if a hardware error exists.

4. If a hardware error exists, or if the `slotPowerOff` or `slotPowerOn` fails on the bladed switch, or if errors are encountered again:
  - On the Core Switch 2/64 or SAN Director 2/128, replace the blade FRU.
  - On the SAN Switch 2/32, replace the motherboard FRU.
  - On the HP StorageWorks SAN Switch 2/8V, SAN Switch 2/16V, or SAN Switch 4/32, replace the switch.

## Severity

INFO

# BL-1016

## Message

```
timestamp, [BL-1016], sequence-number,, CRITICAL, system-name, Blade port  
port-number in slot slot-number failed to enable.
```

## Probable cause

The specified blade port failed to get enabled.

## Recommended action

1. Make sure that the blade is seated correctly.
2. If the blade is seated correctly, reboot or power cycle the blade.
3. Run the `systemVerification` command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
4. If the message persists, replace the blade.

## Severity

CRITICAL

---

# Bloom error messages

# BLL-1000

## Message

```
timestamp, [BLL-1000], sequence-number,, CRITICAL, system-name, ASIC  
driver detected Slot slot-number port port-number as faulty (reason:  
reason)
```

## Probable cause

A blade regulation problem was reported on the specified *slot number*. The blade is faulted. All blade register fault codes are associated with BLOOM error messages. This message is always paired with a

BLOOM message that provides more information on the specific error. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

The reason codes are as follows:

- 1 = Available buffer overflow
- 2 = Backend port buffer timeout
- 3 = Backend port got shut down
- 4 = Embedded port buffer timeout
- 5 = Excessive busy mini buffer
- 6 = Excessive RCC VC on E\_Port
- 7 = Excessive RCC VC on FL\_Port
- 8 = Fail detection buffer tag error
- 9 = Fail detection TX parity error
- 10 = EPI CMEM interrupt error
- 11 = CMI interrupt error
- 12 = Interrupt overrun
- 13 = FDET interrupt
- 14 = Interrupt suspended
- 15 = Filter LISTD error
- 16 = Unknown filter LIST error
- 17 = Wait for LPC open state
- 18 = Wait for Old port state
- 19 = Wait for Open init state
- 20 = TX parity error
- 21 = RAM parity error
- 22 = BISR or RAMINIT error

## Recommended action

1. Make sure that the blade is seated correctly.
2. If the blade is seated correctly, reboot or power cycle the blade.
3. Run the `systemVerification` command to verify that the blade does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
4. If the message persists, replace the blade.

## Severity

CRITICAL

---

# Core edge routing module error messages

## CER-1001

### Message

```
timestamp, [CER-1001], sequence-number,, ERROR, system-name, HA Sync  
broken, since standby Advanced Performance Tuning module does not support  
Management Server (FMS).
```

### Probable cause

The HA synchronization between the active and standby control processors (CPs) is broken because downlevel firmware is loaded on the standby CP. .

### Recommended action

Run the `firmwareDownload` command to upgrade the firmware on the standby CP. You can also disable FMS on the active CP.

### Severity

ERROR

---

# Environment monitor error messages

## EM-1001

### Message

```
timestamp, [EM-1001], sequence-number,, CRITICAL, system-name, FRU Id is  
over heating: Shutting down
```

### Probable cause

A field replaceable unit (FRU) is shutting down due to overheating. This is typically due to a faulty fan but can also be caused by the switch environment.

### Recommended action

1. Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.
2. Run the `fanShow` command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at high-enough speed, they should be replaced. Healthy fan speeds are as follows:
  - SAN Director 2/128 fans run at approximately 2500 RPM.
  - Core Switch 2/64 fans run at approximately 2500 RPM.
  - SAN Switch 4/32 fans run at approximately 6000 RPM.
  - SAN Switch 2/32 fans run at approximately 3500 RPM.

- SAN Switch 2/16V fans run at approximately 9000 RPM.
- SAN Switch 2/8V fans run at approximately 5500 RPM.

The SAN Switch 2/8V has three fans, and the SAN Switch 2/16V has four fans. Values for the individual fans may appear in this message, but these parts cannot be replaced. The switch itself is a FRU.

## Severity

CRITICAL

# EM-1002

## Message

```
timestamp, [EM-1002], sequence-number,, CRITICAL, system-name, System
fan(s) status fan-fru
```

## Probable cause

A non-bladed system has overheated and is going to shut down. Before doing so, all fan speeds are dumped to the console.

## Recommended action

1. Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.
2. Run the `fanShow` command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at high enough speed, they should be replaced. Healthy fan speeds are as follows:
  - SAN Director 2/128 fans run at approximately 2500 RPM.
  - Core Switch 2/64 fans run at approximately 2500 RPM.
  - SAN Switch 4/32 fans run at approximately 6000 RPM.
  - SAN Switch 2/32 fans run at approximately 3500 RPM.
  - SAN Switch 2/16V fans run at approximately 9000 RPM.
  - SAN Switch 2/8V fans run at approximately 5500 RPM.

The SAN Switch 2/8V has three fans, and the SAN Switch 2/16V has four fans. Values for the individual fans may display in this message, but these parts cannot be replaced. The switch itself is a FRU.

## Severity

CRITICAL

# EM-1003

## Message

```
timestamp, [EM-1003], sequence-number,, CRITICAL, system-name, FRU-Id has
unknown hardware identifier: FRU is being faulted.
```



## Probable cause

Indicates that a fan FRU header could not be read or is not valid. The FRU is faulted.

## Recommended action

1. On Core Switch 2/64 or SAN Director 2/128, try reseating the specified FRU.
2. Reboot or power cycle the switch.
3. Run the `systemVerification` command to verify that the switch does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
4. On the Core Switch 2/64 and SAN Director 2/128, replace the specified FRU.
5. On the SAN Switch 2/32 and SAN Switch 4/32, replace the motherboard FRU.
6. On the HP StorageWorks SAN Switch 2/8V and SAN Switch 2/16V, replace the switch. These switches do not have FRUs; the switch itself is a FRU.

## Severity

CRITICAL

# EM-1004

## Message

```
timestamp, [EM-1004], sequence-number,, CRITICAL, system-name, FRU-Id  
failed to power on
```

## Probable cause

A FRU failed to power on and is not being used. The type of FRU is specified in the message.

The *FRU ID* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU ID* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

Try reseating the FRU. If this fails to correct the error, replace the unit.

## Severity

CRITICAL

# EM-1005

## Message

```
timestamp, [EM-1005], sequence-number,, CRITICAL, system-name, FRU-Id is  
shutting down
```

## Probable cause

A blade in the specified slot or the switch (for non-bladed switches) is being shut down for environmental reasons; its temperature or voltage is out of range.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed-port-count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

1. Check the environment and make sure the room temperature is within the operational range of the switch. Use the `fanShow` command to verify fans are operating properly. Make sure that airflow is not blocked around the chassis. If the temperature problem is isolated to the blade itself, replace the blade.
2. Voltage problems on a blade are probably a hardware problem on the blade itself; replace the blade.

## Severity

CRITICAL

# EM-1006

## Message

```
timestamp, [EM-1006], sequence-number,, CRITICAL, system-name, FRU-Id has  
faulted. Sensor(s) below minimum limits
```

## Probable cause

The sensors show the voltage is below minimum limits. The blade in the specified slot is being shut down for environmental reasons; the voltage is too low.

## Recommended action

Voltage problems on a blade are likely a hardware problem on the blade itself; replace the blade.

## Severity

CRITICAL

# EM-1007

## Message

```
timestamp, [EM-1007], sequence-number,, CRITICAL, system-name, FRU-Id is  
being reset. Sensor(s) has exceeded max limits
```

## Probable cause

The voltage on a switch has exceeded environmental limits. A reset is sent to the faulty slot or the switch for non-bladed switches.

## Recommended action

1. A voltage hardware problem may exist on the blade or motherboard of the switch.
2. For the Core Switch 2/64 and SAN Director 2/128, replace the blade FRU.
3. For the SAN Switch 2/32, replace the motherboard FRU.
4. For the HP StorageWorks SAN Switch 2/8V, SAN Switch 2/16V, and SAN Switch 4/32 you must replace the switch.

## Severity

CRITICAL

# EM-1008

## Message

```
timestamp, [EM-1008], sequence-number,, CRITICAL, system-name,  
Incompatible unit in FRU-Id is being faulted
```

## Probable cause

A FRU inserted in the specified slot is not compatible with the switch software. The blade is not used. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

Replace the blade. Make sure the replacement is compatible with your switch type.

## Severity

CRITICAL

# EM-1009

## Message

```
timestamp, [EM-1009], sequence-number,, CRITICAL, system-name, FRU-Id  
powered down unexpectedly
```

## Probable cause

The environmental monitor (EM) received an unexpected power-down notification from the specified FRU. This may indicate a hardware malfunction in the FRU. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

Try reseating the blade. If this fails to correct the error, replace the FRU unit.

## Severity

CRITICAL

## EM-1010

### Message

```
timestamp, [EM-1010], sequence-number,, CRITICAL, system-name, Received  
unexpected power down for FRU-Id But FRU-Id still has power
```

### Probable cause

The environmental monitor received an unexpected power-down notification from the specified FRU. However, the specified FRU still appears to be powered up after four seconds. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

### Recommended action

Try reseating the blade. If this fails to correct the error, replace the FRU unit.

### Severity

CRITICAL

## EM-1011

### Message

```
timestamp, [EM-1011], sequence-number,, CRITICAL, system-name, Can not  
determine if FRU-Id has powered down
```

### Probable cause

The environmental monitor (EM) received an unexpected power-down notification from the FRU specified; however, after four seconds the monitor cannot determine whether the FRU has powered down. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

### Recommended action

Try reseating the blade. If this fails to correct the error, replace the unit.

### Severity

CRITICAL

## EM-1012

### Message

```
timestamp, [EM-1012], sequence-number,, CRITICAL, system-name, FRU-Id  
failed state transition
```

### Probable cause

A switch blade failed to transition from one state to another. It is faulted. The specific failed target *state* is displayed in the message. Serious internal Fabric OS configuration or hardware problems exist on the switch.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

1. On Core Switch 2/64 and SAN Director 2/128, try reseating the indicated FRU.
2. If the message persists, reboot or power cycle the switch.
3. Run the `systemVerification` command to verify that the switch does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
4. If the message persists, replace the FRU.

## Severity

CRITICAL

# EM-1013

## Message

```
timestamp, [EM-1013], sequence-number,, ERROR, system-name, Failed to  
update FRU information for FRU-Id
```

## Probable cause

The environmental monitor was unable to update the time alive or OEM data in the memory on a FRU.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

If the `fruInfoSet` command was being run, try the command again; otherwise, the update is automatically reattempted. If it continues to fail, try reseating the FRU.

If the message persists, replace the unit.

## Severity

ERROR

# EM-1014

## Message

```
timestamp, [EM-1014], sequence-number,, ERROR, system-name, Unable to read  
sensor on FRU-Id (return-code)
```

## Probable cause

The environmental monitor was unable to access the sensors on the specified FRU.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

If the message persists, replace the unit.

## Severity

ERROR

## EM-1015

### Message

```
timestamp, [EM-1015], sequence-number,, WARNING, system-name, Warm  
recovery failed (Return-code)
```

### Probable cause

A problem was discovered when performing consistency checks during a warm boot.

### Recommended action

Perform a `reboot` or power cycle to clear the problem.

### Severity

WARNING

## EM-1016

### Message

```
timestamp, [EM-1016], sequence-number,, WARNING, system-name, Cold  
recovery failed (Return-code)
```

### Probable cause

Consistency checks during a cold boot discovered a problem.

### Recommended action

1. Monitor the switch.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

WARNING

## EM-1017

### Message

```
timestamp, [EM-1017], sequence-number,, WARNING, system-name, Uncommitted  
WWN change detected. Cold reboot required.
```

### Probable cause

A user did not commit a changed WWN value before executing a `reboot`, power cycle, or `firmwareDownload` operation.



## Recommended action

Change and commit the new WWN value.

## Severity

WARNING

# EM-1028

## Message

```
timestamp, [EM-1028], sequence-number,, ERROR, system-name, HIL Error:  
function failed to access FRU: FRU-Id (rc=return-code).
```

## Probable cause

Problems were encountered when the software attempted to write to the memory of the FRU specified in the error message. The return code is for internal use only. This is a serious FRU hardware problem.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64 SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

1. Try reseating the FRU, if possible.
2. If this fails to correct the error, replace the specified unit.

## Severity

ERROR

# EM-1029

## Message

```
timestamp, [EM-1029], sequence-number,, ERROR, system-name, FRU-Id I2C  
access problems (error-code): state current-state
```

## Probable cause

Indicates that the I2C bus had problems and a timeout occurred.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

This is often a transient error.

1. Watch for the EM-1048 message, which indicates that the problem has been resolved.
2. If the error persists, check for loose or dirty connections. Remove all dust and debris prior to reseating the FRU.
3. If it continues to fail, replace the unit.

## Severity

ERROR

# EM-1031

## Message

```
timestamp, [EM-1031], sequence-number,, ERROR, system-name, FRU-Id ejector  
not closed
```

## Probable cause

The environmental monitor (EM) found a switch blade that is inserted, but at least one ejector switch is not latched. The blade in the specified slot is treated as not inserted. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

Close the ejector switch if the FRU is intended for use.

## Severity

ERROR

# EM-1033

## Message

```
timestamp, [EM-1033], sequence-number,, ERROR, system-name, CP in FRU-Id  
set to faulty because CP ERROR asserted
```

## Probable cause

The standby CP has been detected as faulty. The High Availability feature is not available. This message occurs every time the other CP reboots, even as part of a clean warm failover. In most situations, this message is followed by the EM-1047 message, and no action is required for the CP; however, you may want to find out why the failover occurred. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

1. If the standby CP was just rebooted, wait for the error to clear; run `slotShow` to determine whether it has cleared. Watch for the EM-1047 message to verify this error cleared.
2. If the standby CP continues to be faulty or if it was not intentionally rebooted, check the error logs on the other CP (using the `errDump` command) to determine the cause of the error state.
3. If the state persists, try reseating the FRU.
4. If the message persists, replace the FRU.

## Severity

ERROR

# EM-1034

## Message

```
timestamp, [EM-1034], sequence-number,, ERROR, system-name, FRU-Id set to  
faulty, rc=return-code
```

## Probable cause

The specified FRU has been marked as faulty for the specified reason.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

1. Try reseating the FRU.
2. Run the `systemVerification` command to verify that the switch does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
3. If the fault persists, replace the FRU.

## Severity

ERROR

# EM-1036

## Message

```
timestamp, [EM-1036], sequence-number,, WARNING, system-name,  
FRU-Id is not accessible.
```

## Probable cause

The specified FRU does not seem to be present on the switch.

If the FRU is a WWN card, then default WWN and IP addresses are used for the switch.

## Recommended action

1. Reseat the FRU card.
2. If the message persists, reboot or power cycle the switch.
3. Run the `systemVerification` command to verify that the switch does not have hardware problems. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on this command.
4. If the message persists, replace the FRU.

## Severity

WARNING

# EM-1041

## Message

```
timestamp, [EM-1041], sequence-number,, WARNING, system-name, Sensor  
values for FRU-Id: Sensor-Value Sensor-Value Sensor-Value Sensor-Value  
Sensor-Value Sensor-Value Sensor-Value
```

## Probable cause

Sensors detected a warning condition. All significant sensors for the FRU are displayed; each contains a header.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

This message can display:

- Voltages in volts
- Temperature in degrees Celsius
- Fan speeds in RPMs

## Recommended action

If the message is isolated, monitor the error messages on the switch. If the message is associated with other messages, follow the recommended action for those messages.

## Severity

WARNING

# EM-1042

## Message

```
timestamp, [EM-1042], sequence-number,, WARNING, system-name, Important  
FRU header data for FRU-Id is not valid).
```

## Probable cause

The indicated FRU has an incorrect number of sensors in its FRU header-derived information. This could mean that the FRU header was corrupted or read incorrectly or corrupted in the object database, which contains information about all FRUs.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

1. Try reseating the FRU.
2. If the condition persists, replace the FRU unit.

## Severity

WARNING

# EM-1043

## Message

```
timestamp, [EM-1043], sequence-number,, WARNING, system-name, Can't power  
FRU-Id state (on or off).
```

## Probable cause

The specified FRU cannot be powered on or off.

## Recommended action

The specified FRU is not responding to commands and should be replaced.

## Severity

WARNING

# EM-1044

## Message

```
timestamp, [EM-1044], sequence-number,, WARNING, system-name, Can't power on FRU-Id, its logical switch is shut down
```

## Probable cause

The specified FRU cannot be powered on because the associated logical switch is shut down.

## Recommended action

Run the `switchStart` command on the associated logical switch.

## Severity

WARNING

# EM-1045

## Message

```
timestamp, [EM-1045], sequence-number,, WARNING, system-name, FRU-Id is being powered new-state
```

## Probable cause

An automatic power adjustment is being made because of the (predicted) failure of a power supply or the insertion or removal of a port blade. If *new\_state* is *On*, a port blade is being powered on because more power is available (either a power supply was inserted or a port blade was removed or powered down).

If *new\_state* is *Off*, a port blade has been powered down because a power supply has been faulted, because it is indicating a predicted failure.

If *new\_state* is *Down* (not enough power), a newly inserted port blade was not powered on because insufficient power is available.

## Recommended action

The Core Switch 2/64 requires two power supplies for a fully populated chassis; however, you should always operate the system with four operating power supplies for redundancy.

The SAN Director 2/128 requires only a single power supply for a fully populated chassis; however, you should always operate the system with at least two power supplies for redundancy.

## Severity

WARNING

# EM-1046

## Message

```
timestamp, [EM-1046], sequence-number,, WARNING, system-name, Sysctrl  
reports error status for blade ID id-value for the blade in slot  
slot-number
```

## Probable cause

The system controller encountered a blade with an unknown ID in the slot specified. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

If the blade ID listed is not correct, then the FRU header for the blade is corrupted and the blade must be replaced. For the Core Switch 2/64, the blade ID should be 1 for a CP blade and 2 for a port blade. For the SAN Director 2/128, the blade ID should be 5 for a CP blade and 4 for a port blade.

## Severity

WARNING

# EM-1047

## Message

```
timestamp, [EM-1047], sequence-number,, INFO, system-name, CP in slot  
slot-number not faulty, CP ERROR deasserted
```

## Probable cause

The EM-1033 message has been turned off. The new standby CP is in the process of rebooting and has turned off the CP\_ERR signal. This message occurs only on the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

No action is required.

## Severity

INFO



# EM-1048

## Message

```
timestamp, [EM-1048], sequence-number,, INFO, system-name, FRU-Id I2C  
access recovered: state current-state
```

## Probable cause

The I2C bus problems have been resolved and I2C access to the FRU has become available again.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

The EM-1029 error can be a transitory error; if the problem resolves, the EM-1048 message is displayed.

## Severity

INFO

# EM-1049

## Message

```
timestamp, [EM-1049], sequence-number,, INFO, system-name, FRU FRU-Id  
insertion detected.
```

## Probable cause

Indicates that a FRU of the type and location specified by the *FRU ID* was detected as having been inserted into the chassis.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.

- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

Verify that the unit is in service.

## Severity

INFO

# EM-1050

## Message

```
timestamp, [EM-1050], sequence-number,, INFO, system-name, FRU FRU-Id
removal detected.
```

## Probable cause

Indicates that a FRU of the specified type and location was removed from the chassis.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- WWN 1 or WWN 2 for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

Verify that the unit was intended to be removed. Replace the unit as soon as possible.

## Severity

INFO

# EM-1051

## Message

```
timestamp, [EM-1051], sequence-number,, INFO, system-name, FRU-Id:  
Inconsistency detected, FRU re-initialized
```

## Probable cause

An inconsistent state was found in the FRU. This occurs if the state of the FRU was changing during a failover. The FRU is reinitialized and traffic may have been disrupted.

## Recommended action

No action is required.

## Severity

INFO

# EM-1052

## Message

```
timestamp, [EM-1052], sequence-number,, WARNING, system-name,  
FRU-Id sensor 0xSensor-code value out of range:  
Raw-sensor-value/Retry-count
```

## Probable cause

One or more sensor values for a FRU are radically out of range. This may be a environmental problem or a problem with the sensor hardware.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.

- `WWN 1` or `WWN 2` for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

This message can display:

- Voltage in volts
- Temperature in degrees Celsius
- Fan speeds in RPMs

## Recommended action

If the message is isolated, it may be a transient problem with the sensor hardware; monitor the error messages on the switch. If the message is persistent, without other environmental errors, replace the FRU.

If the message is persistent, and other associated environmental messages are displayed, follow the actions for those messages.

## Severity

WARNING

# EM-1053

## Message

```
timestamp, [EM-1053], sequence-number, , WARNING, system-name, No cached
sensor values available for FRU-Id
```

## Probable cause

No cached sensor values exist for the sensor and software was unable to read new values.

The *FRU-Id* value is composed of a FRU-type string and an optional number to identify the unit, slot, or port. The *FRU-Id* value can be:

- Switch for fixed port count switches.
- Slot 1 through Slot 10 for the Core Switch 2/64 and SAN Director 2/128.
- PS 1 through PS 4 (power supplies) for the Core Switch 2/64 and SAN Director 2/128, or PS 1 through PS 2 for the SAN Switch 2/32 and SAN Switch 4/32. The power supplies on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- Fan 1 through Fan 3 for the Core Switch 2/64, SAN Director 2/128, and SAN Switch 4/32 (six fans in three FRUs). Fan 1 through Fan 6 for the SAN Switch 2/32 (six fans in three FRUs). The fans on the SAN Switch 2/8V and the SAN Switch 2/16V are not field replaceable.
- `WWN 1` or `WWN 2` for the Core Switch 2/64 and SAN Director 2/128. Only bladed switches have removable WWN cards. All other switches have a non-removable WWN component on the main logic board.

The SAN Switch 2/8V has one power supply and three fans, and the SAN Switch 2/16V has two power supplies and four fans. Values for the individual fans and power supplies for these switches may appear, but these parts cannot be replaced. The switch itself is a FRU.

## Recommended action

If the message is isolated, it may be a transient problem with the sensor hardware; monitor the error messages on the switch.

If the message is persistent, replace the FRU.

## Severity

WARNING

# EM-1055

## Message

```
timestamp, [EM-1055], sequence-number,, WARNING, system-name,  
FRU-Id: Port media incompatible. Reason: Reason-for-incompatibility
```

## Probable cause

An incompatible port media has been detected.

The possible causes are:

- The port media is not capable of running at the configured port speed.
- The port media generates too much heat to be used in the slot.

## Recommended action

1. Verify that the media can be run at the configured port speed.
2. If the port media is extended long wavelength, move it to a port that can support the heat generated.

## Severity

WARNING

# EM-1056

## Message

```
timestamp, [EM-1056], sequence-number,, WARNING, system-name,  
FRU-Id: Port faulted. Reason: Reason-code-for-the-fault
```

## Probable cause

A faulty port media has been detected. The reason code for this message is for internal use only. This message is valid only for the SAN Switch 4/32.

## Recommended action

Replace the defective port media.

## Severity

WARNING

---

# Event management module error messages

## EVMD-1001

### Message

```
timestamp, [EVMD-1001], sequence-number,, WARNING, system-name, Event  
session killed, host IP = Host-IP-address, port = Host-TCP-port-number
```

### Probable cause

The TCP socket is closed because of a TCP write error. Possible causes for this loss of connection include the following:

- The API host application exits without notifying the switch.
- The API host computer is shut down.
- A network problem exists.
- The Ethernet cable is not properly connected to the switch.
- A user has unplugged the Ethernet cable and then plugged it back in.

### Recommended action

This problem can be transient; try to reestablish the connection.

If the cause is a network or Ethernet cable problem, you must fix the problem before you can reestablish an API session. Verify that your workstation has a TCP connection to the switch.

The Fabric OS automatically kills unused sessions to prevent resource leaking.

## Severity

WARNING

---

# Fabric error messages

## FABR-1001

### Message

```
timestamp, [FABR-1001], sequence-number,, WARNING, system-name, port  
port-number, segmentation-reason
```

## Probable cause

The specified switch port is isolated because of a segmentation due to mismatched configuration parameters.

## Recommended action

1. Based on the segmentation reason displayed with the message, look for a possible mismatch of relevant configuration parameters in the switches at both ends of the link.
2. Run the `configure` command to modify the appropriate switch parameters on both the local and remote switch.

## Severity

WARNING

# FABR-1002

## Message

```
timestamp, [FABR-1002], sequence-number,, WARNING, system-name, fabGaid:  
no free multicast alias IDs
```

## Probable cause

The fabric does not have any available multicast alias IDs to assign to the alias server.

## Recommended action

Verify alias IDs using the `fabricShow` command on the principal switch.

## Severity

WARNING

# FABR-1003

## Message

```
timestamp, [FABR-1003], sequence-number,, WARNING, system-name, port  
port-number: ILS command bad size payload-size, wanted  
expected-payload-size
```

## Probable cause

An internal link service (ILS) information unit of invalid size has been received. The neighbor switch has sent an invalid sized payload.

## Recommended action

1. Investigate the neighbor switch for problems. Run the `errShow` command on the neighbor switch to view the error log for additional messages.
2. Check for a faulty cable or deteriorated SFP. Replace the cable or SFP if necessary.
3. Run the `portLogDumpPort` command on both the receiving and transmitting ports.

4. Run the `fabStateShow` command on both the receiving and transmitting switches.
5. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
6. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# FABR-1004

## Message

```
timestamp, [FABR-1004], sequence-number,, WARNING, system-name, port:  
port-number, req iu: 0xaddress-of-IU-request-sent, state: 0xcommand-sent,  
resp iu: 0xaddress-of-response-IU-received, state 0xresponse-IU-state,  
additional-description
```

## Probable cause

The information unit response is invalid for the specified command sent. The fabric received an unknown response. This message is rare and usually indicates a problem with the Fabric OS kernel.

## Recommended action

If this message is due to a one-time event because of the incoming data, the system discards the frame. If it is due to problems with the kernel, the system recovers by performing a failover.

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# FABR-1005

## Message

```
timestamp, [FABR-1005], sequence-number,, WARNING, system-name,  
command-sent: port port-number: status 0xreason-for-failure  
(description-of-failure-reason) xid = 0xexchange-ID-of-command
```

## Probable cause

The application failed to send an async command for the specified port. The message provides additional details regarding the reason for the failure and the exchange ID of the command. This can occur if a port is about to go down.

## Recommended action

This message is often transitory. No action is required.

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.



## Severity

WARNING

# FABR-1006

## Message

```
timestamp, [FABR-1006], sequence-number,, WARNING, system-name, Node free  
error, caller: error-description
```

## Probable cause

Fabric OS is trying to free or deallocate memory space that has already been deallocated. This message is rare and usually indicates a problem with Fabric OS.

## Recommended action

In case of severe memory corruption, the system may recover by performing an automatic failover.

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# FABR-1007

## Message

```
timestamp, [FABR-1007], sequence-number,, WARNING, system-name, IU free  
error, caller: function-attempting-to-deallocate-IU
```

## Probable cause

A failure occurred when deallocating an information unit. This message is rare and usually indicates a problem with Fabric OS.

## Recommended action

In case of severe memory corruption, the system may recover by performing an automatic failover.

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# FABR-1008

## Message

```
timestamp, [FABR-1008], sequence-number,, WARNING, system-name,  
error-description
```

## Probable cause

Errors occurred during the request domain ID state; the information unit cannot be allocated or sent. If this message occurs with FABR-1005, the problem is usually transitory. Otherwise, this message is rare and usually indicates a problem with Fabric OS. The error descriptions are as follows:

- FAB RDI: cannot allocate IU
- FAB RDI: cannot send IU

## Recommended action

No action is required if the message appears with the FABR\_1005 message.

1. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
2. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# FABR-1009

## Message

```
timestamp, [FABR-1009], sequence-number,, WARNING, system-name,  
error-description
```

## Probable cause

Errors were reported during the exchange fabric parameter state; cannot allocate domain list due to a faulty EFP type. This message is rare and usually indicates a problem with Fabric OS.

## Recommended action

The fabric daemon discards the EFP. The system recovers through the EFP retrieval process.

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# FABR-1010

## Message

```
timestamp, [FABR-1010], sequence-number,, WARNING, system-name,  
error-description
```

## Probable cause

Errors occurred while cleaning up the RDI (request domain ID). The error description provides further details. This message is rare and usually indicates a problem with Fabric OS.

## Recommended action

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# FABR-1011

## Message

```
timestamp, [FABR-1011], sequence-number,, ERROR, system-name,  
error-description
```

## Probable cause

Fabric OS is unable to inform the Fabric OS State Synchronization Management (FSSME) module that the fabric is stable or unstable. This message is rare and usually indicates a problem with Fabric OS.

## Recommended action

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# FABR-1012

## Message

```
timestamp, [FABR-1012], sequence-number,, WARNING, system-name,  
function-stream: no such type, invalid-type
```

## Probable cause

The fabric is not in the appropriate state for the specified process. This message is rare and usually indicates a problem with Fabric OS.

## Recommended action

The fabric daemon takes proper action to recover from the error.

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# FABR-1013

## Message

```
timestamp, [FABR-1013], sequence-number,, CRITICAL, system-name, No  
Memory: pid=fabric-process-ID file=source-file-name  
line=line-number-within-the-source-file
```

## Probable cause

The switch has insufficient memory for the fabric module to allocate. This message is rare and usually indicates a problem with Fabric OS.

## Recommended action

The system recovers by failing over to the standby CP.

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

CRITICAL

# FABR-1014

## Message

```
timestamp, [FABR-1014], sequence-number,, ERROR, system-name, Port  
port-number Disabled: Insistent Domain ID domain-ID could not be obtained.  
Principal Assigned Domain ID = domain-ID
```

## Probable cause

The specified port received an RDI (request domain ID) accept message containing a principal-switch-assigned domain ID that is different from the insistent domain ID (IDID). If an RDI response has a different domain ID, then the port is disabled.

## Recommended action

1. Run the `configShow` command to view the `fabric.ididmode`.  
A value of 0 means the IDID mode is disabled; a value of 1 means it is enabled.
2. Set the switch to insistent domain ID mode. This mode is set under the `configure` command or in Web Tools on the **Switch Admin > configure** window.

## Severity

ERROR

# FABR-1015

## Message

```
timestamp, [FABR-1015], sequence-number,, ERROR, system-name, Insistent  
DID max retry exceeded: All E-Ports will be disabled. Switch is isolated.
```

## Probable cause

The application exceeded RDI (request domain ID) requests for the insistent domain ID. All E\_Ports are disabled, isolating the specified switch from the fabric.

## Recommended action

Verify that the insistent domain ID is unique in the fabric and then reenables the E\_Ports. Run the `fabricShow` command to view the domain IDs across the fabric and the `configure` command to change the insistent domain ID mode. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information on these commands.

## Severity

ERROR

# FABR-1018

## Message

```
timestamp, [FABR-1018], sequence-number,, WARNING, system-name, PSS  
principal failed (reason-for-not-becoming-the-principal-switch:  
WWN-of-new-principal-switch)
```

## Probable cause

A failure occurred during attempt to set the principal switch using the `fabricPrincipal` command. The message notifies the user that the switch failed to become the principal switch due to one of the following reasons:

- The switch joined an existing fabric and bypassed the F0 state.
- The fabric already contains a principal switch that has a lower WWN.

## Recommended action

1. Make sure that no other switches are configured as the principal switch.
2. Force a fabric rebuild by using the `switchDisable` and `switchEnable` commands.

Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information the `fabricPrincipal` command.

## Severity

WARNING

# FABR-1019

## Message

```
timestamp, [FABR-1019], sequence-number,, CRITICAL, system-name, Critical  
fabric size (current-domains) exceeds supported configuration  
(supported-domains)
```

## Probable cause

The switch is a value-line switch and has exceeded the limited fabric size; that is, a specified limit to the number of domains. This limit is defined by your specific value-line license key. The fabric size exceeds this specified limit and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

## Recommended action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

## Severity

CRITICAL

# FABR-1020

## Message

```
timestamp, [FABR-1020], sequence-number,, CRITICAL, system-name, Webtool  
will be disabled in #days days #hours hours and #minutes minutes
```

## Probable cause

The switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This message displays the number of days, hours, and minutes remaining in the grace period. After this time, Web Tools is disabled.

## Recommended action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

## Severity

CRITICAL

# FABR-1021

## Message

```
timestamp, [FABR-1021], sequence-number,, CRITICAL, system-name, Webtool  
is disabled
```

## Probable cause

The switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This grace period expired and Web Tools is disabled.

## Recommended action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

## Severity

CRITICAL

# FABR-1022

## Message

```
timestamp, [FABR-1022], sequence-number,, CRITICAL, system-name, Fabric  
size (actual-domains) exceeds supported configuration (supported-domains).  
Fabric limit timer (type) started from grace-period-in-seconds.
```

## Probable cause

The fabric size exceeds the value-line limit and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

## Recommended action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

## Severity

CRITICAL

# FABR-1023

## Message

```
timestamp, [FABR-1023], sequence-number,, INFO, system-name, Fabric size  
is within supported configuration (supported-domains). Fabric limit timer  
(type) stopped at grace-period-in-seconds.
```

## Probable cause

The fabric size is within specified limits. Either a full fabric license was added or the size of the fabric was changed to within the licensed limit.

## Recommended action

No action is required.

## Severity

INFO

# FABR-1024

## Message

```
timestamp, [FABR-1024], sequence-number,, INFO, system-name, Initializing  
fabric size limit timer grace-period
```

## Probable cause

The fabric size exceeds the limit set by your value-line switches. Value-line switches have a limited fabric size, a specified limit to the number of domains. This value is defined by your specific value-line license key. The fabric size exceeds this specified limit. The grace-period timer has been initialized. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

## Recommended action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

## Severity

INFO

# FABR-1029

## Message

```
timestamp, [FABR-1029], sequence-number,, INFO, system-name, Port  
port-number negotiated flow-control-mode-description (mode =  
received-flow-control-mode)
```

## Probable cause

A different flow control mode, as described in the message, is negotiated with the port at the other end of the link. The flow control is a mechanism of throttling the transmitter port to avoid buffer overrun at the receiving port. The following are three types of flow control modes:

- VC\_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.
- R\_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, which uses R\_RDY primitive for flow control.



- DUAL\_CR mode: Dual-credit flow control mode. In both of the previous modes, the buffer credits are fixed, based on the port configuration information. In this mode, the buffer credits are negotiated as part of ELP exchange. This mode also uses the R\_RDY primitive for flow control.

### Recommended action

No action is required.

### Severity

INFO

---

## Fabric OS system driver module error messages

### FABS-1001

#### Message

```
timestamp, [FABS-1001], sequence-number,, CRITICAL, system-name,  
function-name description-of-memory-need
```

#### Probable cause

The system is low on memory and cannot allocate more memory for new operations. This is usually an internal Fabric OS problem or file corruption. The variable `description-of-memory-need` indicates the amount requested as a whole number.

#### Recommended action

Reboot or power cycle the switch.

#### Severity

CRITICAL

### FABS-1002

#### Message

```
timestamp, [FABS-1002], sequence-number,, WARNING, system-name,  
function-name description-of-problem
```

#### Probable cause

An internal problem has been detected by the software. This is usually an internal Fabric OS problem or file corruption.

#### Recommended action

1. Reboot or power cycle the switch.
2. If the message persists, run the `firmwareDownload` command to update the firmware.

## Severity

WARNING

# FABS-1004

## Message

```
timestamp, [FABS-1004], sequence-number,, WARNING, system-name,  
function-name-and-description-of-problem process process-ID-number  
(current-command-name) pending-signal-number
```

## Probable cause

An operation has been interrupted by a signal. This is usually an internal Fabric OS problem or file corruption.

## Recommended action

Reboot or power cycle the switch.

## Severity

WARNING

# FABS-1005

## Message

```
timestamp, [FABS-1005], sequence-number,, WARNING, system-name,  
function-name-and-description-of-problem (ID-type= ID-number)
```

## Probable cause

An unsupported operation has been requested. This is usually an internal Fabric OS problem or file corruption. The possible values for *function-name-and-description-of-problem* are:

```
fabsys_write: Unsupported write operation: process xxx
```

where *xxx* is the process ID (PID), expressed as a whole number.

## Recommended action

1. Reboot or power cycle the active CP (for modular systems) or the switch (for single-board systems).
2. If the message persists, run the `firmwareDownload` command to update the firmware.

## Severity

WARNING

# FABS-1006

## Message

```
timestamp, [FABS-1006], sequence-number,, WARNING, system-name,  
function-name-and-description-of-problem: object object-type-ID unit slot
```

## Probable cause

There is no device in the slot with the specified object type ID in the system module record. This could indicate that a serious Fabric OS data problem on the switch. The possible values for *function-name-and-description-of-problem* are:

- setSoftState: bad object
- setSoftState: invalid type or unit
- media\_sync: Media OID mapping failed
- fabsys\_media\_i2c\_op: Media OID mapping failed
- fabsys\_media\_i2c\_op: object is not media type
- media\_class\_hndlr: failed sending media state to blade driver

## Recommended action

1. If the message is isolated, monitor the error messages on the switch.
2. If the error is repetitive or if the fabric failed, fail over or reboot the switch.
3. If the message persists, run the `firmwareDownload` command to update the firmware.

## Severity

WARNING

# FABS-1007

## Message

```
timestamp, [FABS-1007], sequence-number,, WARNING, system-name,  
function-name: Media state is invalid - status=status-value
```

## Probable cause

Fabric OS has detected an invalid value in an object's status field. This is usually an internal Fabric OS problem or file corruption.

## Recommended action

1. Reboot or power cycle the switch.
2. If the message persists, run the `firmwareDownload` command to update the firmware.

## Severity

WARNING

# FABS-1008

## Message

```
timestamp, [FABS-1008], sequence-number,, WARNING, system-name,  
function-name: Media oid mapping failed
```

## Probable cause

Fabric OS was unable to locate a necessary object handle. This is usually an internal Fabric OS problem or file corruption.

## Recommended action

Reboot or power cycle the switch.

## Severity

WARNING

# FABS-1009

## Message

```
timestamp, [FABS-1009], sequence-number,, WARNING, system-name,  
function-name: type is not media
```

## Probable cause

Fabric OS was unable to locate an appropriate object handle. This is usually an internal Fabric OS problem or file corruption.

## Recommended action

Reboot or power cycle the switch.

## Severity

WARNING

# FABS-1010

## Message

```
timestamp, [FABS-1010], sequence-number,, WARNING, system-name,  
function-name: Wrong media_event event-number
```

## Probable cause

Fabric OS has detected an unknown event type. This is usually an internal Fabric OS problem or file corruption.

## Recommended action

1. Reboot or power cycle the switch.

2. If the message persists, run the `firmwareDownload` command to update the firmware.

## Severity

WARNING

---

# Fibre Channel miscellaneous error messages

## FCMC-1001

### Message

```
timestamp, [FCMC-1001], sequence-number,, CRITICAL, system-name, function:  
failed-function-call failed, out of memory condition
```

### Probable cause

The switch is low on memory and failed to allocate new memory for an information unit (IU).

### Recommended action

A non-bladed switch reboots. For a bladed switch, the active CP blade fails over and the standby CP becomes the active CP.

## Severity

CRITICAL

---

# Fibre Channel protocol daemon error messages

## FCPD-1001

### Message

```
timestamp, [FCPD-1001], sequence-number,, WARNING, system-name, Probing  
failed on error-string
```

### Probable cause

An FCP switch probed devices on a loop port; probing failed on either the L\_Port, AL\_PA address, or the F\_Port. For the AL\_PA, the valid range is 00 through FF. The error string can be either:

- `L_Port port_number ALPA alpa_number`
- `F_Port port_number`

### Recommended action

This can happen when the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

The SAN Switch 4/32 does not support private loop devices.

## Severity

WARNING

# FCPD-1002

## Message

```
timestamp, [FCPD-1002], sequence-number,, WARNING, system-name, port  
port-number, bad R_CTL for fcp probing: 0xR_CTL-value
```

## Probable cause

The response frame received on the specified port for an inquiry request contains an invalid value in the routing control field.

## Recommended action

This can happen only if the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

## Severity

WARNING

# FCPD-1003

## Message

```
timestamp, [FCPD-1003], sequence-number,, INFO, system-name, Probing  
failed on error-string which is possibly a private device which is not  
supported in this port type
```

## Probable cause

Private devices do not respond to the switch port login (PLOGI) during probing.

## Recommended action

Refer to the switch vendor for a list of other port types that support private devices for inclusion into the fabric.

## Severity

INFO

---

# Fibre Channel physical layer error messages

## FCPH-1001

### Message

```
timestamp, [FCPH-1001], sequence-number,, CRITICAL, system-name, function:  
failed-function-call failed, out of memory condition
```

### Probable cause

The switch is low on memory and failed to allocate new memory for a Fibre Channel driver instance.

The *function* can only be `fc_create`. This function creates a Fibre Channel driver instance.

The *failed-function-call* is `kmalloc_wrapper failed`. This function call is for kernel memory allocation.

### Recommended action

A non-bladed switch reboots. For a bladed switch, the active CP blade fails over and the standby CP becomes the active CP.

### Severity

CRITICAL

---

# Fabric OS I/O kernel library module error messages

## FKLB-1001

### Message

```
timestamp, [FKLB-1001], sequence-number,, WARNING, system-name, exchange  
xid overlapped, pid=pid
```

### Probable cause

The FC kernel driver has timed out the exchange while the application is still active. When the FC kernel driver reuses the exchange, the application overlaps. This happens on a timed-out exchange; it recovers after the application times the exchange out.

### Recommended action

No action is required.

### Severity

WARNING

---

# FLOOD error messages

## FLOD-1001

### Message

```
timestamp, [FLOD-1001], sequence-number,, WARNING, system-name, Unknown  
LSR type: port port-number, type LSR-header-type
```

### Probable cause

The link state record (LSR) type is unknown. The only LSR header types are 1 for Unicast and 3 for Multicast.

### Recommended action

No action is required. The record is discarded.

### Severity

WARNING

## FLOD-1003

### Message

```
timestamp, [FLOD-1003], sequence-number,, WARNING, system-name, Link count  
exceeded in received LSR, value = link-count-number
```

### Probable cause

The acceptable link count received is exceeded in the link state record (LSR).

### Recommended action

No action is required. The record is discarded.

### Severity

WARNING

## FLOD-1004

### Message

```
timestamp, [FLOD-1004], sequence-number,, ERROR, system-name, Excessive  
LSU length = LSU-length
```



## Probable cause

The LSU size exceeds what the system can support.

## Recommended action

Reduce the number of switches in the fabric or reduce the number of redundant intersite links (ISLs) between two switches.

## Severity

ERROR

# FLOD-1005

## Message

```
timestamp, [FLOD-1005], sequence-number,, WARNING, system-name, Invalid  
received domain ID: domain-number
```

## Probable cause

The received LSR contained an invalid domain number.

## Recommended action

No action is required. The LSR is discarded.

## Severity

WARNING

# FLOD-1006

## Message

```
timestamp, [FLOD-1006], sequence-number,, WARNING, system-name,  
Transmitting invalid domain ID: domain-number
```

## Probable cause

The transmit LSR contains an invalid domain number.

## Recommended action

No action is required. The LSR is discarded.

## Severity

WARNING

---

# Fabric shortest path first error messages

## FSPF-1001

### Message

```
timestamp, [FSPF-1001], sequence-number,, ERROR, system-name, Input Port  
port-number out of range
```

### Probable cause

The specified input port number is out of range; it does not exist on the switch.

### Recommended action

No action is required.

### Severity

ERROR

## FSPF-1002

### Message

```
timestamp, [FSPF-1002], sequence-number,, INFO, system-name, Wrong  
neighbor ID (domain-ID) in Hello message from port port-number, expected  
ID = domain-ID
```

### Probable cause

The switch received the wrong domain ID from an adjacent switch in the HELLO message from a specified port. This may happen when a domain ID for a switch is changed.

### Recommended action

No action is required.

### Severity

INFO

## FSPF-1003

### Message

```
timestamp, [FSPF-1003], sequence-number,, ERROR, system-name, Remote  
Domain ID domain-number out of range, input port = port-number
```

### Probable cause

The specified remote domain ID is out of range.

## Recommended action

No action is required. The frame is discarded.

## Severity

ERROR

# FSPF-1005

## Message

```
timestamp, [FSPF-1005], sequence-number,, ERROR, system-name, Wrong  
Section Id section-number, should be section-number, input port =  
port-number
```

## Probable cause

An incorrect section ID has been reported from the specified input port. The section ID identifies a set of switches that share an identical topology database. The section ID is implemented inside the protocol. The error message itself indicates the mismatched section ID. It should be set to 0 for a non hierarchical fabric. HP StorageWorks switches support only section ID 0.

## Recommended action

Use a frame analyzer to verify that the reported section ID is 0. Any connected (other manufacturer) switch with a section ID other than 0 is incompatible in a fabric of HP StorageWorks switches. Disconnect the offending switch.

## Severity

ERROR

# FSPF-1006

## Message

```
timestamp, [FSPF-1006], sequence-number,, ERROR, system-name,  
FSPF Version FSPF-version not supported, input port = port-number
```

## Probable cause

The FSPF version is not supported on the specified input port.

## Recommended action

Update the FSPF version by running the `firmwareDownload` command to update the firmware to the latest version. All current versions of the Fabric OS support FSPF version 2, which is the correct version.

## Severity

ERROR

---

# Fabric OS state synchronization framework error messages

## FSS-1001

### Message

```
timestamp, [FSS-1001], sequence-number,, WARNING, system-name, Application dropping HA data update.
```

### Probable cause

An application dropped a high-availability (HA) data update.

### Recommended action

1. Run the `haSyncStart` command if the system is a dual-CP system; reboot the switch if it is a non-bladed system.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

WARNING

## FSS-1002

### Message

```
timestamp, [FSS-1002], sequence-number,, WARNING, system-name, Application sending too many concurrent HA data updates
```

### Probable cause

An application sent too many concurrent high-availability (HA) data updates.

### Recommended action

1. Run the `haSyncStart` command if the system is a dual-CP system; reboot the switch if it is a non-bladed system.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

WARNING

## FSS-1003

### Message

```
timestamp, [FSS-1003], sequence-number,, WARNING, system-name, Application  
missing first HA data update
```

### Probable cause

The FSS has dropped the update because an application has not set the transaction flag correctly.

### Recommended action

1. Run the `haSyncStart` command if the system is a dual-CP system; reboot the switch if it is a non-bladed system.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

WARNING

## FSS-1004

### Message

```
timestamp, [FSS-1004], sequence-number,, ERROR, system-name, Memory  
shortage
```

### Probable cause

The system ran out of memory.

### Recommended action

1. Run the `memShow` command to view memory usage.
2. Run the `haSyncStart` command if the system is a dual-CP system; reboot the switch if it is a non-bladed system.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

### Severity

ERROR

## FSS-1005

### Message

```
timestamp, [FSS-1005], sequence-number,, WARNING, system-name, FSS read  
failure
```

## Probable cause

The read system call to the FSS device failed.

## Recommended action

Run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# FSS-1006

## Message

```
timestamp, [FSS-1006], sequence-number,, WARNING, system-name, No message available
```

## Probable cause

Data is not available on the FSS device.

## Recommended action

Run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

---

# Fabric OS state synchronization management module error messages

# FSSM-1002

## Message

```
timestamp, [FSSM-1002], sequence-number,, INFO, system-name, HA State is in sync
```

## Probable cause

The high-availability (HA) state for the active CP is in synchronization with the HA state of the standby CP. If the standby CP is healthy, a failover is nondisruptive. For more information on the `haFailover` command, refer to the *HP StorageWorks Fabric OS 4.x command reference guide*.

## Recommended action

No action is required.

## Severity

INFO

# FSSM-1003

## Message

```
timestamp, [FSSM-1003], sequence-number,, WARNING, system-name, HA State  
out of sync
```

## Probable cause

The high-availability (HA) state for the active CP is out of synchronization with the HA state of the standby CP. If the active CP failover occurs when the HA state is out of sync, the failover is disruptive.

## Recommended action

If this message was logged as a result of a user-initiated action (such as running the `switchReboot` command), then no action is required.

1. Otherwise, issue the `haSyncStart` command on the active CP and try resynchronizing the HA state.
2. If the HA state does not become synchronized, run the `haDump` command to diagnose the problem.

## Severity

WARNING

# FSSM-1004

## Message

```
timestamp, [FSSM-1004], sequence-number,, CRITICAL, system-name, Active  
and the standby CP have incompatible software.
```

## Probable cause

The active CP and the standby CP are running firmware incompatible with each other. If the active CP fails, the failover is disruptive.

## Recommended action

Run the `firmwareDownload` command to load compatible firmware on the standby CP. For details on this command, refer to the *HP StorageWorks Fabric OS 4.x command reference guide*.

## Severity

CRITICAL

---

# Fabric Watch module error messages

## FW-1001

### Message

```
timestamp, [FW-1001], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The internal temperature of the switch changed.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

1. To prevent recurring messages, disable the changed alarm for this threshold.
2. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance.
3. If all fans are functioning normally, check the climate control in your lab.

### Severity

INFO

## FW-1002

### Message

```
timestamp, [FW-1002], sequence-number,, WARNING, system-name, label, is  
below low boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

### Probable cause

The internal temperature of the switch has fallen below the low boundary.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation. Typically, low temperatures mean that the fans and airflow of a switch are functioning normally.

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

### Severity

WARNING



## FW-1003

### Message

```
timestamp, [FW-1003], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The internal temperature of the switch rose above the high boundary to a value that may damage the switch. This message generally appears when a fan fails. If so, a fan-failure message accompanies this message.

### Recommended action

Replace the fan.

### Severity

WARNING

## FW-1004

### Message

```
timestamp, [FW-1004], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The internal temperature of the switch has changed from a value outside the acceptable range to a value within the acceptable range.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

### Severity

INFO

## FW-1005

### Message

```
timestamp, [FW-1005], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The speed of the fan has changed. Fan problems usually contribute to temperature problems. Consistently abnormal fan speeds generally indicate that the fan is malfunctioning.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1006

## Message

```
timestamp, [FW-1006], sequence-number,, WARNING, system-name, label, is  
below low boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The speed of the fan has fallen below the low boundary. Fan problems usually contribute to temperature problems. Consistently abnormal fan speeds generally indicate that the fan is failing.

## Recommended action

Replace the fan FRU.

## Severity

WARNING

# FW-1007

## Message

```
timestamp, [FW-1007], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The speed of the fan has risen above the high boundary. Fan problems usually contribute to temperature problems. Consistently abnormal fan speeds generally indicate that the fan is failing.

## Recommended action

Replace the fan FRU.

## Severity

WARNING

## FW-1008

### Message

```
timestamp, [FW-1008], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The speed of the fan has changed from a value outside the acceptable range to a value within the acceptable range. Fan problems usually contribute to temperature problems. Consistently abnormal fan speeds generally indicate that the fan is failing.

### Recommended action

No action is required. If this message occurs repeatedly, replace the fan FRU.

### Severity

INFO

## FW-1009

### Message

```
timestamp, [FW-1009], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The state of the power supply has changed from faulty to functional or from functional to faulty.

### Recommended action

If the power supply is functioning correctly, no action is required.

1. If the power supply is functioning below the acceptable boundary, verify that it is seated correctly in the chassis.
2. Run the `psShow` command to view the status of the power supply.
3. If the power supply continues to be a problem, replace it.

### Severity

INFO

# FW-1010

## Message

```
timestamp, [FW-1010], sequence-number,, WARNING, system-name, label, is  
below low boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The power supply is faulty. It is not producing enough power.

## Recommended action

1. Verify that you have installed the power supply correctly and that it is correctly seated in the chassis.
2. If the problem persists, replace the faulty power supply.

## Severity

WARNING

# FW-1011

## Message

```
timestamp, [FW-1011], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The power supply is functioning properly.

## Recommended action

Set the high boundary above the normal operation range.

## Severity

INFO

# FW-1012

## Message

```
timestamp, [FW-1012], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The power supply counter changed from a value outside the acceptable range to a value within the acceptable range.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1033

## Message

```
timestamp, [FW-1033], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The temperature of the SFP changed.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation. Frequent fluctuations in SFP temperature may indicate a deteriorating SFP.

## Severity

INFO

# FW-1034

## Message

```
timestamp, [FW-1034], sequence-number,, WARNING, system-name, label, is  
below low boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The temperature of the SFP fell below the low boundary.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

WARNING

## FW-1035

### Message

```
timestamp, [FW-1035], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The temperature of the SFP rose above the high boundary. Frequent fluctuations in temperature may indicate a deteriorating SFP.

### Recommended action

Replace the SFP.

### Severity

WARNING

## FW-1036

### Message

```
timestamp, [FW-1036], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The temperature of the SFP changed from a value outside the acceptable range to a value within the acceptable range. Frequent fluctuations in temperature may indicate a deteriorating SFP.

### Recommended action

No action is required.

### Severity

INFO

## FW-1037

### Message

```
timestamp, [FW-1037], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The receive power value of the SFP changed. The receive performance area measures the amount of incoming laser to help determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating. Incoming laser fluctuations usually indicate a deteriorating SFP.

## Recommended action

If this message occurs repeatedly, replace the SFP.

## Severity

INFO

# FW-1038

## Message

```
timestamp, [FW-1038], sequence-number,, WARNING, system-name, label, is  
below low boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The receive power value of the SFP fell below the low boundary. The receive performance area measures the amount of incoming laser to help determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

## Recommended action

1. Verify that your optical components are clean and function properly.
2. Check for damage from heat or age.
3. Replace deteriorating cables or SFPs.

## Severity

WARNING

# FW-1039

## Message

```
timestamp, [FW-1039], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The receive power value of the SFP rose above the high boundary. The receive performance area measures the amount of incoming laser to help determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

## Recommended action

Replace the SFP before it deteriorates.

## Severity

WARNING

## FW-1040

### Message

```
timestamp, [FW-1040], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The receive power value of the SFP changed from a value outside the acceptable range to a value within the acceptable range. The receive performance area measures the amount of incoming laser to help determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1041

### Message

```
timestamp, [FW-1041], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The transmit power value of the SFP changed. The transmit-performance area measures the amount of outgoing laser to help determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating. Transmitting laser fluctuations usually indicates a deteriorating SFP.

### Recommended action

If this message occurs repeatedly, replace the SFP.

### Severity

INFO

## FW-1042

### Message

```
timestamp, [FW-1042], sequence-number,, WARNING, system-name, label, is  
below low boundary(High=high-value, Low=low-value). Current value is value  
unit.
```



## Probable cause

The transmit power value of the SFP fell below the low boundary. The transmit-performance area measures the amount of outgoing laser to help determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

## Recommended action

1. Verify that your optical components are clean and function properly.
2. Check for damage from heat or age.
3. Replace deteriorating cables or SFPs.

## Severity

WARNING

# FW-1043

## Message

```
timestamp, [FW-1043], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The transmit power value of the SFP rose above the high boundary. The transmit-performance area measures the amount of outgoing laser to help determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

## Recommended action

Replace the SFP.

## Severity

WARNING

# FW-1044

## Message

```
timestamp, [FW-1044], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The transmit power value of the SFP changed from a value outside the acceptable range to a value within the acceptable range. The transmit-performance area measures the amount of outgoing laser to help determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1045

## Message

```
timestamp, [FW-1045], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The value of the SFP voltage changed. If the supplied voltage of the SFP transceiver is outside the normal range, this may indicate a hardware failure.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation. Frequent messages indicate that you must replace the SFP.

## Severity

INFO

# FW-1046

## Message

```
timestamp, [FW-1046], sequence-number,, WARNING, system-name, label, is  
below low boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The value of the SFP voltage fell below the low boundary.

## Recommended action

1. Verify that your optical components are clean and function properly.
2. Check for damage from heat or age.
3. Replace deteriorating cables or SFPs.

## Severity

WARNING

## FW-1047

### Message

```
timestamp, [FW-1047], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The value of the SFP voltage rose above the high boundary. The supplied current of the SFP transceiver is outside the normal range, indicating possible hardware failure.

### Recommended action

Replace the SFP.

### Severity

WARNING

## FW-1048

### Message

```
timestamp, [FW-1048], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The value of the SFP voltage changed from a value outside the acceptable range to a value within the acceptable range.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1049

### Message

```
timestamp, [FW-1049], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The value of the SFP voltage changed. Frequent voltage fluctuations are an indication that the SFP is deteriorating.

## Recommended action

Replace the SFP.

## Severity

INFO

# FW-1050

## Message

```
timestamp, [FW-1050], sequence-number,, WARNING, system-name, label, is  
below low boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The SFP voltage fell below the low boundary.

## Recommended action

1. Configure the low threshold to 1 so that the threshold triggers an alarm when the value falls to 0 (Out\_of\_Range).
2. If continuous or repeated alarms occur, replace the SFP before it deteriorates.

## Severity

WARNING

# FW-1051

## Message

```
timestamp, [FW-1051], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The value of the SFP voltage has risen above the high boundary. High voltages indicate possible hardware failures. Frequent voltage fluctuations are an indication that the SFP is deteriorating.

## Recommended action

Replace the SFP.

## Severity

WARNING

## FW-1052

### Message

```
timestamp, [FW-1052], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The value of the SFP voltage changed from a value outside the acceptable range to a value within the acceptable range.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1113

### Message

```
timestamp, [FW-1113], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of times E\_Ports have gone down has changed. E\_Ports go down each time you remove a cable or SFP. SFP failures also cause E\_Ports to go down. E\_Ports going down may be caused by transient errors.

### Recommended action

Check both ends of the physical connection and verify that the SFPs and cables are functioning properly.

### Severity

INFO

## FW-1114

### Message

```
timestamp, [FW-1114], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of times E\_Ports have gone down has fallen below the low boundary. E\_Ports go down each time you remove a cable or SFP. SFP failures also cause E\_Ports to go down. E\_Ports going down may be caused by transient errors. A low number of E\_Port failures means that the switch is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1115

## Message

```
timestamp, [FW-1115], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The number of times E\_Ports have gone down has risen above the high boundary. E\_Ports go down each time you remove a cable or SFP. SFP failures also cause E\_Ports to go down. E\_Ports going down may be caused by transient errors.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation. Check both ends of the physical connection and verify that the SFP functions properly.

## Severity

INFO

# FW-1116

## Message

```
timestamp, [FW-1116], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of times E\_Ports have gone down has changed from a value outside the acceptable range to a value within the acceptable range. E\_Ports go down each time you remove a cable or SFP. SFP failures also cause E\_Ports to go down. E\_Ports going down may be caused by transient errors.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1117

## Message

```
timestamp, [FW-1117], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of fabric reconfigurations changed. The following actions can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics are joined.
- An E\_Port went offline.
- A principal link segmented from the fabric.

## Recommended action

An inexplicable fabric reconfiguration may be a transient error and may not require troubleshooting.

1. Verify that the cable is properly connected at both ends.
2. Verify that the SFPs have not become faulty.

## Severity

INFO

# FW-1118

## Message

```
timestamp, [FW-1118], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of fabric reconfigurations fell below the low boundary. A low number of fabric reconfigurations means that the fabric is functioning normally. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID are connected to one another.
- Two fabrics are joined.
- An E\_Port went offline.
- A principal link segmented from the fabric.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1119

## Message

```
timestamp, [FW-1119], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The number of fabric reconfigurations rose above the high boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID are connected to one another.
- Two fabrics are joined.
- An E\_Port went offline.
- A principal link segmented from the fabric.

## Recommended action

An inexplicable fabric reconfiguration may be a transient error and may not require troubleshooting.

1. Verify that all ISL cables are properly connected at both ends.
2. Verify that the SFP has not become faulty.

## Severity

INFO

# FW-1120

## Message

```
timestamp, [FW-1120], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of fabric reconfigurations has changed from a value outside the acceptable range to a value within the acceptable range. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID are connected to one another.
- Two fabrics are joined.



- An E\_Port went offline.
- A principal link segmented from the fabric.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1121

## Message

```
timestamp, [FW-1121], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of domain ID changes changed. Domain ID changes occur when a conflict of domain IDs occur in a single fabric and the principal switch has to assign another domain ID to the switch.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1122

## Message

```
timestamp, [FW-1122], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of domain ID changes fell below the low boundary. Domain ID changes occur when a conflict of domain IDs occur in a single fabric and the principal switch has to assign another domain ID to the switch. A low number of domain ID changes means that the fabric is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

## FW-1123

### Message

```
timestamp, [FW-1123], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

### Probable cause

The number of domain ID changes rose above the high boundary. Domain ID changes occur when a conflict of domain IDs occur in a single fabric and the principal switch has to assign another domain ID to the switch.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1124

### Message

```
timestamp, [FW-1124], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of domain ID changes changed from a value outside the acceptable range to a value within the acceptable range. Domain ID changes occur when a conflict of domain IDs occur in a single fabric and the principal switch has to assign another domain ID to the switch.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1125

### Message

```
timestamp, [FW-1125], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of segmentations changed. Segmentation changes may occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E\_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1126

## Message

```
timestamp, [FW-1126], sequence-number, , INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of segmentations fell below the low boundary. Segmentation changes may occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E\_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation. A low number of segmentation errors means that the fabric is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1127

## Message

```
timestamp, [FW-1127], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The number of segmentations rose above the high boundary. Segmentation changes may occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E\_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1128

## Message

```
timestamp, [FW-1128], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of segmentations changed from a value outside the acceptable range to a value within the acceptable range. Segmentation changes may occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E\_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1129

## Message

```
timestamp, [FW-1129], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of zone changes changed. Zone changes occur when a change is made to the effective zone configuration.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1130

## Message

```
timestamp, [FW-1130], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of zone changes fell below the low boundary. Zone changes occur when a change is made to the effective zone configuration. A low number of zone configuration changes means that the fabric is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

## FW-1131

### Message

```
timestamp, [FW-1131], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

### Probable cause

The number of zone changes rose above the high boundary. Zone changes occur when a change is made to the effective zone configuration.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1132

### Message

```
timestamp, [FW-1132], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of zone changes changed from a value outside the acceptable range to a value within the acceptable range. Zone changes occur when a change is made to the effective zone configuration.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1133

### Message

```
timestamp, [FW-1133], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of fabric logins changed. Fabric logins occur when a port or device initializes with the fabric. The event is called a *fabric login* or *FLOGI*.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1134

## Message

```
timestamp, [FW-1134], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of fabric logins fell below the low boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a *fabric login* or *FLOGI*. A low number of fabric logins means that the fabric is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1135

## Message

```
timestamp, [FW-1135], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The number of fabric logins rose above the high boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a *fabric login* or *FLOGI*.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

## FW-1136

### Message

```
timestamp, [FW-1136], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of fabric logins changed from a value outside the acceptable range to a value within the acceptable range. Fabric logins occur when a port or device initializes with the fabric. The event is called a *fabric login* or *FLOGI*.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1137

### Message

```
timestamp, [FW-1137], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of SFP state changes changed. SFP state changes occur when the SFP is inserted or removed.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1138

### Message

```
timestamp, [FW-1138], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of SFP state changes fell below the low boundary. SFP state changes occur when the SFP is inserted or removed. A low number of SFP state changes means that the switch is functioning normally.



## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1139

## Message

```
timestamp, [FW-1139], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The number of SFP state changes rose above the high boundary. SFP state changes occur when the SFP is inserted or removed.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1140

## Message

```
timestamp, [FW-1140], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of SFP state changes changed from a value outside the acceptable range to a value within the acceptable range. SFP state changes occur when the SFP is inserted or removed.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

## FW-1141

### Message

```
timestamp, [FW-1141], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of QuickLoop changes changed.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1142

### Message

```
timestamp, [FW-1142], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of QuickLoop changes fell below the low boundary.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1143

### Message

```
timestamp, [FW-1143], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

### Probable cause

The number of QuickLoop changes rose above the high boundary.

## Recommended action

Verify that the cable is properly connected at both ends. This may be a transient error and may not require troubleshooting.

## Severity

INFO

# FW-1144

## Message

```
timestamp, [FW-1144], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of QuickLoop changes changed from a value outside the acceptable range to a value within the acceptable range.

## Recommended action

Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1160

## Message

```
timestamp, [FW-1160], sequence-number,, INFO, system-name, port-name,  
label, value has changed(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of link failures that the port experiences changed. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss-of-synchronization errors and, if applicable, troubleshoot them.

## Recommended action

1. Check both ends of your cable connection.
2. Verify that the cable and SFPs are not faulty.
3. If you receive concurrent loss-of-synchronization errors, troubleshoot the loss of synchronization.

## Severity

INFO

# FW-1161

## Message

```
timestamp, [FW-1161], sequence-number,, INFO, system-name,  
port-name, label, is below low boundary(High=high-value,  
Low=low-value). Current value is value unit.
```

## Probable cause

The number of link failures that the port experiences fell below the low boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss-of-synchronization errors and, if applicable, troubleshoot them. A low number of link loss errors means that the switch is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1162

## Message

```
timestamp, [FW-1162], sequence-number,, WARNING, system-name,  
port-name, label, is above high boundary(High=high-value,  
Low=low-value). Current value is value unit.
```

## Probable cause

The number of link failures that the port experiences rose above the high boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss-of-synchronization errors and, if applicable, troubleshoot them.

## Recommended action

1. Check both ends of your cable connection.
2. Verify that the cable and SFPs are not faulty.
3. If you receive concurrent loss-of-synchronization errors, troubleshoot the loss of synchronization.

## Severity

WARNING

# FW-1163

## Message

```
timestamp, [FW-1163], sequence-number,, INFO, system-name,  
port-name, label, is between high and low boundaries(High=high-value,  
Low=low-value). Current value is value unit.
```

## Probable cause

The number of link failures that the port experiences changed from a value outside the acceptable range to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Link loss errors frequently occur due to a loss of synchronization.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation. Check for concurrent loss-of-synchronization errors and, if applicable, troubleshoot them.

## Severity

INFO

# FW-1164

## Message

```
timestamp, [FW-1164], sequence-number,, INFO, system-name,  
port-name, label, value has changed(High=high-value, Low=low-value).  
Current value is value unit.
```

## Probable cause

The number of synchronization losses that the port experiences changed. Loss-of-synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

## Recommended action

1. Check both ends of your cable connection.
2. Verify that the cable and SFPs are not faulty.
3. If you continue to experience synchronization loss errors, troubleshoot your HBA and contact your switch service provider.

## Severity

INFO

# FW-1165

## Message

```
timestamp, [FW-1165], sequence-number,, INFO, system-name,  
port-name, label, is below low boundary(High=high-value,  
Low=low-value). Current value is value unit.
```

## Probable cause

The number of synchronization losses that the port experiences fell below the low boundary. Loss-of-synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses. A low number of synchronization losses means that the switch is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1166

## Message

```
timestamp, [FW-1166], sequence-number,, WARNING, system-name,  
port-name, label, is above high boundary(High=high-value, Low=low-value).  
Current value is value unit.
```

## Probable cause

The number of synchronization losses that the port experiences rose above the high boundary. Loss-of-synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

## Recommended action

1. Check both ends of your cable connection.
2. Verify that the cable and SFPs are not faulty.
3. If you continue to experience loss-of-synchronization errors, troubleshoot your HBA and contact your switch service provider.

## Severity

WARNING

## FW-1167

### Message

```
timestamp, [FW-1167], sequence-number,, INFO, system-name,  
port-name, label, is between high and low boundaries (High=high-value,  
Low=low-value). Current value is value unit.
```

### Probable cause

The number of synchronization losses that the port experiences changed from a value outside the acceptable range to a value within the acceptable range. Loss-of-synchronization errors frequently occur due to a faulty SFP or cable. Signal losses often create synchronization losses.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1168

### Message

```
timestamp, [FW-1168], sequence-number,, INFO, system-name,  
port-name, label, value has changed (High=high-value, Low=low-value).  
Current value is value unit.
```

### Probable cause

The number of signal losses that the port experiences changed. Loss of signal generally indicates a physical problem.

### Recommended action

Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

### Severity

INFO

## FW-1169

### Message

```
timestamp, [FW-1169], sequence-number,, INFO, system-name,  
port-name, label, is below low boundary (High=high-value, Low=low-value).  
Current value is value unit.
```

## Probable cause

The number of signal losses that the port experiences fell below the low boundary. Loss of signal generally indicates a physical problem. A low number of signal loss errors means that the switch is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1170

## Message

```
timestamp, [FW-1170], sequence-number,, WARNING, system-name,  
port-name, label, is above high boundary(High=high-value, Low=low-value).  
Current value is value unit.
```

## Probable cause

The number of signal losses that the port experiences rose above the high boundary. Loss of signal generally indicates a physical problem.

## Recommended action

Check both ends of your cable connection and verify that the cable is not faulty.

## Severity

WARNING

# FW-1171

## Message

```
timestamp, [FW-1171], sequence-number,, INFO, system-name,  
port-name, label, is between high and low boundaries(High=high-value,  
Low=low-value). Current value is value unit.
```

## Probable cause

The number of signal losses that the port experiences changed from a value outside the acceptable range to a value within the acceptable range. Loss of signal generally indicates a physical problem. Frequent loss of signal generally indicates a physical problem.

## Recommended action

Respond to this message as is appropriate for the relevant policy of the end-user installation.

Check both ends of your cable connection and verify that the cable and SFPs are not faulty.



## Severity

INFO

# FW-1172

## Message

```
timestamp, [FW-1172], sequence-number,, INFO, system-name,  
port-name, label, value has changed(High=high-value,  
Low=low-value). Current value is value unit.
```

## Probable cause

The number of protocol errors that the port experiences changed. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

## Recommended action

Check both ends of your cable connection and verify that the cable and SFPs are not faulty.

## Severity

INFO

# FW-1173

## Message

```
timestamp, [FW-1173], sequence-number,, INFO, system-name,  
port-name, label, is below low boundary(High=high-value,  
Low=low-value). Current value is value unit.
```

## Probable cause

The number of protocol errors that the port experiences fell below the low boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems. A low number of protocol errors means that the switch is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

## FW-1174

### Message

```
timestamp, [FW-1174], sequence-number,, WARNING, system-name, port-name,  
label, is above high boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of protocol errors that the port experiences rose above the high boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

### Recommended action

Check both ends of your connection and verify that your cable and SFP are not faulty.

### Severity

WARNING

## FW-1175

### Message

```
timestamp, [FW-1175], sequence-number,, INFO, system-name, port-name,  
label, is between high and low boundaries(High=high-value, Low=low-value).  
Current value is value unit.
```

### Probable cause

The number of protocol errors that the port experiences changed from a value outside the acceptable range to a value within the acceptable range. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1176

### Message

```
timestamp, [FW-1176], sequence-number,, INFO, system-name, port-name,  
label, value has changed(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of invalid words that the port experiences changed. Invalid words usually indicate a hardware problem with an SFP or cable.

## Recommended action

Check both ends of your connections, your SFP, and your cable to verify that they are not faulty.

## Severity

INFO

# FW-1177

## Message

```
timestamp, [FW-1177], sequence-number,, INFO, system-name, port-name,  
label, is below low boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of invalid words that the port experiences fell below the low boundary. Invalid words usually indicate a hardware problem with an SFP or cable. A low number of invalid words means that the switch is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1178

## Message

```
timestamp, [FW-1178], sequence-number,, WARNING, system-name, port-name,  
label, is above high boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of invalid words that the port experiences rose above the high boundary. Invalid words usually indicate a hardware problem with an SFP or cable.

## Recommended action

Check both ends of your connections, your SFP, and your cable to verify that they are not faulty.

## Severity

WARNING

## FW-1179

### Message

```
timestamp, [FW-1179], sequence-number,, INFO, system-name, port-name,  
label, is between high and low boundaries (High=high-value, Low=low-value).  
Current value is value unit.
```

### Probable cause

The number of invalid words that the port experiences changed from a value outside the acceptable range to a value within the acceptable range. Invalid words usually indicate a hardware problem with an SFP or cable.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1180

### Message

```
timestamp, [FW-1180], sequence-number,, INFO, system-name, port-name,  
label, value has changed (High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The number of invalid CRCs that the port experiences changed. Frequent fluctuations in CRC errors generally indicate an aging fabric.

### Recommended action

Respond to this message as is appropriate for the relevant policy of the end-user installation.

1. Check your SFPs, cables, and connections for faulty hardware.
2. Verify that all optical hardware is clean.

### Severity

INFO

## FW-1181

### Message

```
timestamp, [FW-1181], sequence-number,, INFO, system-name, port-name,  
label, is below low boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of invalid CRCs that the port experiences fell below the low boundary. A low number of invalid CRCs means that the switch is functioning normally.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1182

### Message

```
timestamp, [FW-1182], sequence-number,, WARNING, system-name, port-name,  
label, is above high boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of invalid CRCs that the port experiences rose above the high boundary. This error generally indicates deteriorating fabric hardware.

### Recommended action

1. Check your SFPs, cables, and connections for faulty hardware.
2. Verify that all optical hardware is clean.

### Severity

WARNING

## FW-1183

### Message

```
timestamp, [FW-1183], sequence-number,, INFO, system-name, port-name,  
label, is between high and low boundaries(High=high-value, Low=low-value).  
Current value is value unit.
```

## Probable cause

The number of invalid CRCs that the port experiences changed from a value outside the acceptable range to a value within the acceptable range. Frequent fluctuations in CRC errors generally indicate an aging fabric.

## Recommended action

Respond to this message as is appropriate for the relevant policy of the end-user installation.

1. Check your SFPs, cables, and connections for faulty hardware.
2. Verify that all optical hardware is clean.

## Severity

INFO

# FW-1184

## Message

```
timestamp, [FW-1184], sequence-number,, INFO, system-name, port-name,  
label, value has changed(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The percentage of incoming traffic that the port experiences changed.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1185

## Message

```
timestamp, [FW-1185], sequence-number,, INFO, system-name, port-name,  
label, is below low boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The percentage of incoming traffic that the port experiences fell below the low boundary.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1186

## Message

```
timestamp, [FW-1186], sequence-number,, INFO, system-name, port-name,  
label, is above high boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The percentage of incoming traffic that the port experiences rose above the high boundary.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1187

## Message

```
timestamp, [FW-1187], sequence-number,, INFO, system-name, port-name,  
label, is between high and low boundaries(High=high-value, Low=low-value).  
Current value is value unit.
```

## Probable cause

The percentage of incoming traffic that the port experiences changed from a value outside the acceptable range to a value within the acceptable range.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

## FW-1188

### Message

```
timestamp, [FW-1188], sequence-number,, INFO, system-name, port-name,  
label, value has changed(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The percentage of outgoing traffic that the port experiences changed.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1189

### Message

```
timestamp, [FW-1189], sequence-number,, INFO, system-name, port-name,  
label, is below low boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The percentage of outgoing traffic that the port experiences fell below the low boundary.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1190

### Message

```
timestamp, [FW-1190], sequence-number,, INFO, system-name, port-name,  
label, is above high boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The percentage of outgoing traffic that the port experiences rose above the high boundary.



## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1191

## Message

```
timestamp, [FW-1191], sequence-number,, INFO, system-name, port-name,  
label, is between high and low boundaries(High=high-value, Low=low-value).  
Current value is value unit.
```

## Probable cause

The percentage of outgoing traffic that the port experiences changed from a value outside the acceptable range to a value within the acceptable range.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1192

## Message

```
timestamp, [FW-1192], sequence-number,, INFO, system-name, port-name,  
label, value has changed(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of state changes that the port experiences changed. The state of the port has changed for one of the following reasons; the port:

- Has gone offline
- Has come online
- Is testing
- Is faulty
- Has become an E\_Port
- Has become an F\_Port
- Has segmented

- Has become a trunk port

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1193

## Message

```
timestamp, [FW-1193], sequence-number,, INFO, system-name, port-name,  
label, is below low boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of state changes that the port experiences fell below the low boundary. A low number of port state changes means that the switch is functioning normally. The state of the port has changed for one of the following reasons; the port:

- Has gone offline
- Has come online
- Is testing
- Is faulty
- Has become an E\_Port
- Has become an F\_Port
- Has segmented
- Has become a trunk port.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1194

## Message

```
timestamp, [FW-1194], sequence-number,, WARNING, system-name, port-name,  
label, is above high boundary(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of state changes that the port experiences rose above the high boundary. The state of the port has changed for one of the following reasons; the port:

- Has gone offline
- Has come online
- Is testing
- Is faulty
- Has become an E\_Port
- Has become an F\_Port
- Has segmented
- Has become a trunk port.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

WARNING

# FW-1195

## Message

```
timestamp, [FW-1195], sequence-number,, INFO, system-name, port-name,  
label, is between high and low boundaries (High=high-value, Low=low-value).  
Current value is value unit.
```

## Probable cause

The number of state changes that the port experiences changed from a value outside the acceptable range to a value within the acceptable range. The state of the port has changed for one of the following reasons; the port:

- Has gone offline
- Has come online
- Is testing
- Is faulty
- Has become an E\_Port
- Has become an F\_Port
- Has segmented
- Has become a trunk port

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1216

## Message

```
timestamp, [FW-1216], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of AL\_PA CRC errors changed. This indicates that errors were detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages may also be caused by dirty equipment, temperature fluctuations, and aging equipment.

## Recommended action

1. Set your high boundaries to five- or six-digit figures; only large numbers of messages indicate a problem in this area.
2. Verify that your optical components are clean and function properly.
3. Check for damage from heat and age.
4. Replace deteriorating cables or SFPs.

## Severity

INFO

# FW-1217

## Message

```
timestamp, [FW-1217], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of AL\_PA CRC errors fell below the low boundary. This indicates that errors were detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages may also be caused by dirty equipment, temperature fluctuations, and aging equipment. A low level of invalid CRC errors means that the switch is functioning normally.

## Recommended action

Set your high boundaries to five- or six-digit figures; only large numbers of messages indicate a problem in this area. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1218

## Message

```
timestamp, [FW-1218], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of CRC errors rose above the high boundary. This indicates that errors were detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages may also be caused by dirty equipment, temperature fluctuations, and aging equipment.

## Recommended action

1. Set your high boundaries to five- or six-digit figures; only large numbers of messages indicate a problem in this area.
2. When an above-the-boundary message is received, check for a faulty cable or deteriorated SFP.
3. Replace the cable or SFP if necessary.
4. Try cleaning the connectors.
5. Check for damage from heat and deterioration from age.

## Severity

WARNING

# FW-1219

## Message

```
timestamp, [FW-1219], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of CRC errors changed from a value outside the acceptable range to a value within the acceptable range. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages may also be caused by dirty equipment, temperature fluctuations, and aging equipment.

## Recommended action

Respond to this message as is appropriate for the relevant policy of the end-user installation. Set your high boundaries to five- or six-digit figures; only large numbers of messages indicate a problem in this area.

## Severity

INFO

# FW-1240

## Message

```
timestamp, [FW-1240], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of EE CRC errors changed. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages may also be caused by dirty equipment, temperature fluctuations, and aging equipment.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1241

## Message

```
timestamp, [FW-1241], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of EE CRC errors fell below the low boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages may also be caused by dirty equipment, temperature fluctuations, and aging equipment. A low number of CRC errors means that the fabric is functioning normally.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation. The CRC error area of the End-to-End Performance Monitor class helps you tune your fabric. To reduce CRC messages, experiment with alternative topologies and cabling schemes.

## Severity

INFO

# FW-1242

## Message

```
timestamp, [FW-1242], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of EE CRC errors rose above the high boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages may also be caused by dirty equipment, temperature fluctuations, and aging equipment.

## Recommended action

The CRC error area of the End-to-End Performance Monitor class helps the user tune the fabric. To reduce CRC errors, experiment with alternative topologies and cabling schemes. Clean equipment, check temperatures, and replace old hardware.

## Severity

WARNING

# FW-1243

## Message

```
timestamp, [FW-1243], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of EE CRC errors changed from a value outside the acceptable range to a value within the acceptable range. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S\_ID) and destination ID (D\_ID) pairs change. These messages may also be caused by dirty equipment, temperature fluctuations, and aging equipment.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

## FW-1244

### Message

```
timestamp, [FW-1244], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of EE word frames that the switch receives changed. Receive-performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1245

### Message

```
timestamp, [FW-1245], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of EE word frames that the switch receives fell below the low boundary. Receive-performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1246

### Message

```
timestamp, [FW-1246], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```



## Probable cause

The number of EE word frames that the switch receives rose above the high boundary. Receive-performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1247

## Message

```
timestamp, [FW-1247], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of EE word frames that the switch receives changed from a value outside the acceptable range to a value within the acceptable range. Receive-performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1248

## Message

```
timestamp, [FW-1248], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of EE word frames that the switch transmits changed. Transmit-performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1249

## Message

```
timestamp, [FW-1249], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of EE word frames that the switch transmits fell below the low boundary.  
Transmit-performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1250

## Message

```
timestamp, [FW-1250], sequence-number,, INFO, system-name, label, is above  
high boundary(High=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The number of EE word frames that the switch transmits rose above the high boundary.  
Transmit-performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

## FW-1251

### Message

```
timestamp, [FW-1251], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of EE word frames that the switch transmits changed from a value outside the acceptable range to a value within the acceptable range. Transmit-performance messages appear due to the number of word frames that travel from the configured S\_ID to the D\_ID pair.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1272

### Message

```
timestamp, [FW-1272], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of frame types or commands that the port receives changed. The port received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1273

### Message

```
timestamp, [FW-1273], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of frame types or commands that the port receives fell below the low boundary. The port received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1274

## Message

```
timestamp, [FW-1274], sequence-number,, INFO, system-name, label, is above  
high boundary(High=Filter-counter, Low=Low-value). Current value is value  
unit.
```

## Probable cause

The number of frame types or commands that the port receives rose above the high boundary. The port received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1275

## Message

```
timestamp, [FW-1275], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of frame types or commands that the port receives changed from a value outside the acceptable range to a value within the acceptable range. The port received SCSI Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1296

## Message

```
timestamp, [FW-1296], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of telnet violations changed. Telnet violations indicate that a telnet connection request was received from an unauthorized IP address. The TELNET\_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard dot notation (for example, 255.255.255.255).

## Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

# FW-1297

## Message

```
timestamp, [FW-1297], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of telnet violations fell below the low boundary. Telnet violations indicate that a telnet connection request was received from an unauthorized IP address. The TELNET\_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard dot notation (for example, 255.255.255.255).

## Recommended action

No action is required.

## Severity

INFO

## FW-1298

### Message

```
timestamp, [FW-1298], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The number of telnet violations rose above the high boundary. Telnet violations indicate that a telnet connection request was received from an unauthorized IP address. The TELNET\_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard dot notation (for example, 255.255.255.255).

### Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1299

### Message

```
timestamp, [FW-1299], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of telnet violations changed from a value outside the acceptable range to a value within the acceptable range. Telnet violations indicate that a telnet connection request was received from an unauthorized IP address. The TELNET\_POLICY contains a list of TCP/IP addresses that are authorized to establish telnet connections to switches in the fabric. The IP addresses use standard dot notation (for example, 255.255.255.255).

### Recommended action

No action is required.

### Severity

INFO

## FW-1300

### Message

```
timestamp, [FW-1300], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of HTTP violations changed. HTTP violations indicate that a browser connection request was received from an unauthorized IP address. The HTTP\_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard dot notation (for example, 255.255.255.255).

### Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1301

### Message

```
timestamp, [FW-1301], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of HTTP violations fell below the low boundary. HTTP violations indicate that a browser connection request was received from an unauthorized IP address. The HTTP\_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard dot notation (for example, 255.255.255.255).

### Recommended action

No action is required.

### Severity

INFO

## FW-1302

### Message

```
timestamp, [FW-1302], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of HTTP violations rose above the high boundary. HTTP violations indicate that a browser connection request was received from an unauthorized IP address. The HTTP\_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard dot notation (for example, 255.255.255.255).

## Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1303

## Message

```
timestamp, [FW-1303], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of HTTP violations changed from a value outside the acceptable range to a value within the acceptable range. HTTP violations indicate that a browser connection request was received from an unauthorized IP address. The HTTP\_POLICY contains a list of TCP/IP addresses that are authorized to establish browser connections to the switches in the fabric. The IP addresses use the standard dot notation (for example, 255.255.255.255).

## Recommended action

No action is required.

## Severity

INFO

# FW-1304

## Message

```
timestamp, [FW-1304], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of API violations changed. API violations indicate that an API connection request was received from an unauthorized IP address. The SNMP\_POLICY contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard dot notation (for example, 255.255.255.255).



## Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

# FW-1305

## Message

```
timestamp, [FW-1305], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of API violations fell below the low boundary. API violations indicate that an API connection request was received from an unauthorized IP address. The `SNMP_POLICY` contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard dot notation (for example, `255.255.255.255`).

## Recommended action

No action is required.

## Severity

INFO

# FW-1306

## Message

```
timestamp, [FW-1306], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of API violations rose above the high boundary. API violations indicate that an API connection request was received from an unauthorized IP address. The `SNMP_POLICY` contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard dot notation (for example, `255.255.255.255`).

## Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

## FW-1307

### Message

```
timestamp, [FW-1307], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of API violations changed from a value outside the acceptable range to a value within the acceptable range. API violations indicate that an API connection request was received from an unauthorized IP address. The SNMP\_POLICY contains a list of TCP/IP addresses that are authorized to establish API connections to switches in the fabric. The IP addresses use standard dot notation (for example, 255.255.255.255).

### Recommended action

No action is required.

### Severity

INFO

## FW-1308

### Message

```
timestamp, [FW-1308], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of RSNMP violations changed. RSNMP violations indicate that an SNMP get operation request was received from an unauthorized IP address.

### Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1309

### Message

```
timestamp, [FW-1309], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of RSNMP violations fell below the low boundary. RSNMP violations indicate that an SNMP get operation request was received from an unauthorized IP address.

## Recommended action

No action is required.

## Severity

INFO

# FW-1310

## Message

```
timestamp, [FW-1310], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of RSNMP violations rose above the high boundary. RSNMP violations indicate that an SNMP get operation request was received from an unauthorized IP address.

## Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1311

## Message

```
timestamp, [FW-1311], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of RSNMP violations changed from a value outside the acceptable range to a value within the acceptable range. RSNMP violations indicate that an SNMP get operation request was received from an unauthorized IP address.

## Recommended action

No action is required.

## Severity

INFO

## FW-1312

### Message

```
timestamp, [FW-1312], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of WSNMP violations changed. WSNMP violations indicate that an SNMP get/set operation request was received from an unauthorized IP address.

### Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1313

### Message

```
timestamp, [FW-1313], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of WSNMP violations fell below the low boundary. WSNMP violations indicate that an SNMP get/set operation request was received from an unauthorized IP address.

### Recommended action

No action is required.

### Severity

INFO

## FW-1314

### Message

```
timestamp, [FW-1314], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The number of WSNMP violations rose above the high boundary. WSNMP violations indicate that an SNMP get/set operation request was received from an unauthorized IP address.

## Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1315

## Message

```
timestamp, [FW-1315], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of WSNMP violations changed from a value outside the acceptable range to a value within the acceptable range. WSNMP violations indicate that an SNMP get/set operation request was received from an unauthorized IP address.

## Recommended action

No action is required.

## Severity

INFO

# FW-1316

## Message

```
timestamp, [FW-1316], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of SES violations changed. SES violations indicate that a SCSI Enclosure Services (SES) request was received from an unauthorized WWN. The SES\_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

## Recommended action

Run the `errShow` command to determine the IP address that sent the request. Responses to security class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

## FW-1317

### Message

```
timestamp, [FW-1317], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of SES violations fell below the low boundary. SES violations indicate that a SCSI Enclosure Services (SES) request was received from an unauthorized WWN. The SES\_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

### Recommended action

No action is required.

### Severity

INFO

## FW-1318

### Message

```
timestamp, [FW-1318], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The number of SES violations rose above the high boundary. SES violations indicate that a SCSI Enclosure Services (SES) request was received from an unauthorized WWN. The SES\_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

### Recommended action

Run the `errShow` command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1319

### Message

```
timestamp, [FW-1319], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of SES violations changed from a value outside the acceptable range to a value within the acceptable range. SES violations indicate that a SCSI Enclosure Services (SES) request was received from an unauthorized WWN. The SES\_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

## Recommended action

No action is required.

## Severity

INFO

# FW-1320

## Message

```
timestamp, [FW-1320], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of MS violations changed. MS violations indicate that a Management Server (MS) access request was received from an unauthorized WWN. The MS\_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

## Recommended action

Run the `errShow` command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

# FW-1321

## Message

```
timestamp, [FW-1321], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of MS violations fell below the low boundary. MS violations indicate that a Management Server (MS) access request was received from an unauthorized WWN. The MS\_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

## Recommended action

No action is required.

## Severity

INFO

# FW-1322

## Message

```
timestamp, [FW-1322], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of MS violations rose above the high boundary. MS violations indicate that a Management Server (MS) access request was received from an unauthorized WWN. The MS\_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

## Recommended action

Run the `errShow` command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1323

## Message

```
timestamp, [FW-1323], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of MS violations changed from a value outside the acceptable range to a value within the acceptable range. MS violations indicate that a Management Server (MS) access request was received from an unauthorized WWN. The MS\_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

## Recommended action

No action is required.

## Severity

INFO



## FW-1324

### Message

```
timestamp, [FW-1324], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of serial violations changed. Serial violations indicate that an unauthorized serial port request was received. The SERIAL\_POLICY contains a list of switch WWNs for which serial port access is enabled.

### Recommended action

Run the `errShow` command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1325

### Message

```
timestamp, [FW-1325], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of serial violations fell below the low boundary. Serial violations indicate that an unauthorized serial port request was received. The SERIAL\_POLICY contains a list of switch WWNs for which serial port access is enabled.

### Recommended action

No action is required.

### Severity

INFO

## FW-1326

### Message

```
timestamp, [FW-1326], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of serial violations rose above the high boundary. Serial violations indicate that an unauthorized serial port request was received. The SERIAL\_POLICY contains a list of switch WWNs for which serial port access is enabled.

## Recommended action

Run the `errShow` command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1327

## Message

```
timestamp, [FW-1327], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of serial violations changed from a value outside the acceptable range to a value within the acceptable range. Serial violations indicate that an unauthorized serial port request was received. The SERIAL\_POLICY contains a list of switch WWNs for which serial port access is enabled.

## Recommended action

No action is required.

## Severity

INFO

# FW-1328

## Message

```
timestamp, [FW-1328], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of front panel violations changed. Front panel violations indicate that an unauthorized front panel request was received. The FRONTPANEL\_POLICY contains a list of switch WWNs for which front panel access is enabled.

## Recommended action

Run the `errShow` command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

# FW-1329

## Message

```
timestamp, [FW-1329], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of front panel violations fell below the low boundary. Front panel violations indicate that an unauthorized front panel request was received. The FRONTPANEL\_POLICY contains a list of switch WWNs for which front panel access is enabled.

## Recommended action

No action is required.

## Severity

INFO

# FW-1330

## Message

```
timestamp, [FW-1330], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of front panel violations rose above the high boundary. Front panel violations indicate that an unauthorized front panel request was received. The FRONTPANEL\_POLICY contains a list of switch WWNs for which front panel access is enabled.

## Recommended action

Run the `errShow` command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

## FW-1331

### Message

```
timestamp, [FW-1331], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of front panel violations changed from a value outside the acceptable range to a value within the acceptable range. Front panel violations indicate that an unauthorized front panel request was received. The FRONTPANEL\_POLICY contains a list of switch WWNs for which front panel access is enabled.

### Recommended action

No action is required.

### Severity

INFO

## FW-1332

### Message

```
timestamp, [FW-1332], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of SCC violations changed. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC\_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

### Recommended action

Run the `errShow` command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1333

### Message

```
timestamp, [FW-1333], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of SCC violations fell below the low boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC\_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

## Recommended action

No action is required.

## Severity

INFO

# FW-1334

## Message

```
timestamp, [FW-1334], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of SCC violations rose above the high boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC\_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

## Recommended action

Run the `errShow` command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1335

## Message

```
timestamp, [FW-1335], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of SCC violations changed from a value outside the acceptable range to a value within the acceptable range. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC\_POLICY contains a list of switches by WWN that are allowed to be members of a fabric.

## Recommended action

No action is required.

## Severity

INFO

# FW-1336

## Message

```
timestamp, [FW-1336], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of DCC violations has changed.

DCC violations indicate that an unauthorized device tried to join the fabric. The DCC\_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the Name Server.

## Recommended action

Run the `errShow` command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

# FW-1337

## Message

```
timestamp, [FW-1337], sequence-number,, INFO, system-name, label, is below  
low boundary(HHigh=high-value, Low=low-value). Current value is value  
unit.
```

## Probable cause

The number of DCC violations fell below the low boundary.

DCC violations indicate that an unauthorized device tried to join the fabric. The DCC\_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the Name Server.

## Recommended action

No action is required.

## Severity

INFO

## FW-1338

### Message

```
timestamp, [FW-1338], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The number of DCC violations rose above the high boundary.

DCC violations indicate that an unauthorized device tried to join the fabric. The DCC\_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request that the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the Name Server.

### Recommended action

Run the `errShow` command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1339

### Message

```
timestamp, [FW-1339], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of DCC violations changed from a value outside the acceptable range to a value within the acceptable range.

DCC violations indicate that an unauthorized device tried to join the fabric. The DCC\_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request that the WWN specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

### Recommended action

No action is required.

### Severity

INFO

## FW-1340

### Message

```
timestamp, [FW-1340], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of login violations changed. Login violations indicate that a login failure was detected.

### Recommended action

Run the `errShow` command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1341

### Message

```
timestamp, [FW-1341], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of login violations fell below the low boundary. Login violations indicate that a login failure was detected.

### Recommended action

No action is required.

### Severity

INFO

## FW-1342

### Message

```
timestamp, [FW-1342], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The number of login violations rose above the high boundary. Login violations indicate that a login failure was detected.



## Recommended action

Run the `errShow` command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1343

## Message

```
timestamp, [FW-1343], sequence-number,, INFO, system-name, label,  
is between high and low boundaries(High=high-value, Low=low-value).  
Current value is value unit.
```

## Probable cause

The number of login violations changed from a value outside the acceptable range to a value within the acceptable range. Login violations indicate that a login failure was detected.

## Recommended action

No action is required.

## Severity

INFO

# FW-1344

## Message

```
timestamp, [FW-1344], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of invalid timestamps changed.

Invalid-timestamp violations indicate that a packet with an invalid timestamp was received from the primary fabric configuration server (FCS).

When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, the receiving switch rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

# FW-1345

## Message

```
timestamp, [FW-1345], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of invalid timestamps fell below the low boundary.

Invalid-timestamp violations indicate that a packet with an invalid timestamp was received from the primary fabric configuration server (FCS).

When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, the receiving switch rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

## Recommended action

No action is required.

## Severity

INFO

# FW-1346

## Message

```
timestamp, [FW-1346], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of invalid timestamps rose above the high boundary.

Invalid-timestamp violations indicate that a packet with an invalid timestamp was received from the primary fabric configuration server (FCS).

When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, the receiving switch rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1347

## Message

```
timestamp, [FW-1347], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of invalid timestamps changed from a value outside the acceptable range to a value within the acceptable range.

Invalid-timestamp violations indicate that a packet with an invalid timestamp was received from the primary fabric configuration server (FCS).

When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, the receiving switch rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

## Recommended action

No action is required.

## Severity

INFO

# FW-1348

## Message

```
timestamp, [FW-1348], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of invalid signatures changed.

Invalid-signature violations indicate that a packet with an invalid signature was received from the primary fabric configuration server (FCS).

When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, the receiving switch rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

# FW-1349

## Message

```
timestamp, [FW-1349], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of invalid signatures fell below the low boundary.

Invalid-signature violations indicate that a packet with an invalid signature was received from the primary fabric configuration server (FCS).

When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, the receiving switch rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

## Recommended action

No action is required.

## Severity

INFO

# FW-1350

## Message

```
timestamp, [FW-1350], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of invalid signatures rose above the high boundary.

Invalid-signature violations indicate that a packet with an invalid signature was received from the primary fabric configuration server (FCS).

When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, the receiving switch rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1351

## Message

```
timestamp, [FW-1351], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of invalid signatures changed from a value outside the acceptable range to a value within the acceptable range.

Invalid-signature violations indicate that a packet with an invalid signature was received from the primary fabric configuration server (FCS).

When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, the receiving switch rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

## Recommended action

No action is required.

## Severity

INFO

# FW-1352

## Message

```
timestamp, [FW-1352], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of invalid certificates changed. A packet with an invalid certificate was received from the primary fabric configuration server (FCS).

Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root certificate authority (CA) recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

# FW-1353

## Message

```
timestamp, [FW-1353], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of invalid certificates fell below the low boundary. A packet with an invalid certificate was received from the primary fabric configuration server (FCS).

Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root certificate authority (CA) recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

## Recommended action

No action is required.

## Severity

INFO

# FW-1354

## Message

```
timestamp, [FW-1354], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of invalid certificates rose above the high boundary. A packet with an invalid certificate was received from the primary fabric configuration server (FCS).

Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root certificate authority (CA) recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

## FW-1355

### Message

```
timestamp, [FW-1355], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of invalid certificates changed from a value outside the acceptable range to a value within the acceptable range. A packet with an invalid certificate has been received from the primary fabric configuration server (FCS).

Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root certificate authority (CA) recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

### Recommended action

No action is required.

### Severity

INFO

## FW-1356

### Message

```
timestamp, [FW-1356], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of authentication failures changed.

Authentication failures can occur for many reasons. The switch on the other side may not support the protocol, have an invalid certificate, have a certificate that is not properly signed, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

### Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

# FW-1357

## Message

```
timestamp, [FW-1357], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of authentication failures fell below the low boundary.

Authentication failures can occur for many reasons. The switch on the other side may not support the protocol, have an invalid certificate, have a certificate that is not properly signed, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

## Recommended action

No action is required.

## Severity

INFO

# FW-1358

## Message

```
timestamp, [FW-1358], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of authentication failures rose above the high boundary.

Authentication failures can occur for many reasons. The switch on the other side may not support the protocol, have an invalid certificate, have a certificate that is not properly signed, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING



## FW-1359

### Message

```
timestamp, [FW-1359], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of authentication failures changed from a value outside the acceptable range to a value within the acceptable range.

Authentication failures can occur for many reasons. The switch on the other side may not support the protocol, have an invalid certificate, have a certificate that is not properly signed, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

### Recommended action

No action is required.

### Severity

INFO

## FW-1360

### Message

```
timestamp, [FW-1360], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of SLAP faulty packets changed. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

### Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1361

### Message

```
timestamp, [FW-1361], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of SLAP faulty packets fell below the low boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

## Recommended action

No action is required.

## Severity

INFO

# FW-1362

## Message

```
timestamp, [FW-1362], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of SLAP faulty packets rose above the high boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1363

## Message

```
timestamp, [FW-1363], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of SLAP faulty packets changed from a value outside the acceptable range to a value within the acceptable range. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

## Recommended action

No action is required.

## Severity

INFO

## FW-1364

### Message

```
timestamp, [FW-1364], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of time service (TS) out-of-sync violations changed.

### Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

## FW-1365

### Message

```
timestamp, [FW-1365], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of time service out-of-sync violations fell below the low boundary.

### Recommended action

No action is required.

### Severity

INFO

## FW-1366

### Message

```
timestamp, [FW-1366], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The number of time service (TS) out-of-sync violations rose above the high boundary.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

# FW-1367

## Message

```
timestamp, [FW-1367], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The number of time service (TS) out-of-sync violations changed from a value outside the acceptable range to a value within the acceptable range.

## Recommended action

No action is required.

## Severity

INFO

# FW-1368

## Message

```
timestamp, [FW-1368], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of no-FCS violations changed.

This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that no FCSs exist in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

INFO

## FW-1369

### Message

```
timestamp, [FW-1369], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of no-FCS violations fell below the low boundary.

This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that no FCSs exist in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

### Recommended action

No action is required.

### Severity

INFO

## FW-1370

### Message

```
timestamp, [FW-1370], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The number of no-FCS violations rose above the high boundary.

This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that no FCSs exist in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

### Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1371

### Message

```
timestamp, [FW-1371], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of no-FCS violations changed from a value outside the acceptable range to a value within the acceptable range.

This counter records how often the switch loses contact with the primary FCS switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the WWN of that primary FCS switch. If a secure switch finds that no FCSs exist in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

### Recommended action

No action is required.

### Severity

INFO

## FW-1372

### Message

```
timestamp, [FW-1372], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of incompatible security database violations changed. The number of secure switches with different version stamps has been detected.

When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

### Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO

# FW-1373

## Message

```
timestamp, [FW-1373], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

## Probable cause

The number of incompatible security database violations fell below the low boundary. The number of secure switches with different version stamps was detected.

When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

## Recommended action

No action is required.

## Severity

INFO

# FW-1374

## Message

```
timestamp, [FW-1374], sequence-number,, WARNING, system-name, label,  
is above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

## Probable cause

The number of incompatible security database violations rose above the high boundary. The number of secure switches with different version stamps has been detected.

When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

## Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

## Severity

WARNING

## FW-1375

### Message

```
timestamp, [FW-1375], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of incompatible security database violations changed from a value outside the acceptable range to a value within the acceptable range. The number of secure switches with different version stamps have been detected.

When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

### Recommended action

No action is required.

### Severity

INFO

## FW-1376

### Message

```
timestamp, [FW-1376], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of illegal commands changed.

This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. Many commands can be executed only on the primary FCS switch; one security command can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

### Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

INFO



## FW-1377

### Message

```
timestamp, [FW-1377], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The number of illegal commands fell below the low boundary.

This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. Many commands can be executed only on the primary FCS switch; one security command can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

### Recommended action

No action is required.

### Severity

INFO

## FW-1378

### Message

```
timestamp, [FW-1378], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The number of illegal commands rose above the high boundary.

This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. Many commands can be executed only on the primary FCS switch; one security command can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

### Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

### Severity

WARNING

## FW-1379

### Message

```
timestamp, [FW-1379], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

### Probable cause

The number of illegal commands changed from a value outside the acceptable range to a value within the acceptable range.

This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. Many commands can be executed only on the primary FCS switch; one security command can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

### Recommended action

No action is required.

### Severity

INFO

## FW-1400

### Message

```
timestamp, [FW-1400], sequence-number,, INFO, system-name, label, value  
has changed(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The flash usage percentage changed. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1401

### Message

```
timestamp, [FW-1401], sequence-number,, INFO, system-name, label, is below  
low boundary(High=high-value, Low=low-value). Current value is value unit.
```

### Probable cause

The flash usage percentage fell below the low boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

### Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

### Severity

INFO

## FW-1402

### Message

```
timestamp, [FW-1402], sequence-number,, WARNING, system-name, label, is  
above high boundary(High=high-value, Low=low-value). Current value is  
value unit.
```

### Probable cause

The flash usage percentage rose above the high boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

### Recommended action

1. Consider removing some unwanted files to create more flash space.
2. Run the `saveCore` command to remove files from the kernel space.

### Severity

WARNING

## FW-1403

### Message

```
timestamp, [FW-1403], sequence-number,, INFO, system-name, label, is  
between high and low boundaries(High=high-value, Low=low-value). Current  
value is value unit.
```

## Probable cause

The flash usage percentage changed from a value outside the acceptable range to a value within the acceptable range. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

# FW-1424

## Message

```
timestamp, [FW-1424], sequence-number,, WARNING, system-name, Switch  
status changed from previous-state to current-state.
```

## Probable cause

The switch status is not in a healthy state due to a policy violation.

## Recommended action

Run the `switchStatusShow` command to determine the policy violation.

## Severity

WARNING

# FW-1425

## Message

```
timestamp, [FW-1425], sequence-number,, INFO, system-name, Switch status  
changed from bad-state to HEALTHY.
```

## Probable cause

The switch status changed to a healthy state because a policy is no longer violated.

## Recommended action

No action is required. Respond to this message as is appropriate for the relevant policy of the end-user installation.

## Severity

INFO

## FW-1426

### Message

```
timestamp, [FW-1426], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Power supply: number-bad bad,  
number-missing absent.
```

### Probable cause

The switch status is not in a healthy state because the number of faulty or missing power supplies is greater than or equal to the policy set by the `switchStatusPolicySet` command.

### Recommended action

Replace the faulty or missing power supply.

### Severity

WARNING

## FW-1427

### Message

```
timestamp, [FW-1427], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Power supply: number-bad bad.
```

### Probable cause

The switch status is not in a healthy state because the number of faulty power supplies is greater than or equal to the policy set by the `switchStatusPolicySet` command.

### Recommended action

Replace the faulty power supply.

### Severity

WARNING

## FW-1428

### Message

```
timestamp, [FW-1428], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Power supply:  
number-missing absent.
```

### Probable cause

The switch status is not in a healthy state because the number of missing power supplies is greater than or equal to the policy set by the `switchStatusPolicySet` command.

## Recommended action

Replace the missing power supply.

## Severity

WARNING

# FW-1429

## Message

```
timestamp, [FW-1429], sequence-number,, WARNING, system-name, Switch  
status change contributing factor: Power supplies are not redundant.
```

## Probable cause

The switch status is not in a healthy state because the power supplies are not in the correct slots for redundancy.

## Recommended action

Rearrange the power supplies so that one is in an odd slot and other in an even slot to make them redundant.

## Severity

WARNING

# FW-1430

## Message

```
timestamp, [FW-1430], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Temperature sensor: number-bad bad.
```

## Probable cause

The switch status is not in a healthy state because the number of faulty temperature sensors is greater than or equal to the policy set by the `switchStatusPolicySet` command. A temperature sensor is faulty when the sensor value is not in the acceptable range or is faulty.

## Recommended action

Replace the FRU with the faulty temperature sensor.

## Severity

WARNING

## FW-1431

### Message

```
timestamp, [FW-1431], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Fan: number-bad bad.
```

### Probable cause

The switch status is not in a healthy state because the number of faulty fans is greater than or equal to the policy set by the `switchStatusPolicySet` command. A fan is faulty when sensor value is not in the acceptable range or is faulty.

### Recommended action

Replace the faulty or deteriorating fan FRUs.

### Severity

WARNING

## FW-1432

### Message

```
timestamp, [FW-1432], sequence-number,, WARNING, system-name, Switch  
status change contributing factor WWN: number-bad bad.
```

### Probable cause

The switch status is not in a healthy state because the number of faulty WWN cards is greater than or equal to the policy set by the `switchStatusPolicySet` command.

### Recommended action

Replace the faulty WWN card.

### Severity

WARNING

## FW-1433

### Message

```
timestamp, [FW-1433], sequence-number,, WARNING, system-name, Switch  
status change contributing factor CP: CP non-redundant.
```

## Probable cause

The switch status is not in a healthy state because the number of faulty control processors (CPs) is greater than or equal to the policy set by the `switchStatusPolicySet` command. The CPs are non-redundant.

If you power cycle a SAN Director 2/128 chassis in dual-domain configuration, and then reset the micro-switch of the active CP before the heartbeat is up, both CPs to come up in a non-redundant state.

## Recommended action

1. Run the `firmwareShow` command to verify that both CPs have compatible firmware levels.
2. Run the `firmwareDownload` command to install the same level of firmware to both CPs. Replace any faulty CPs.
3. If you reset the micro-switch (the latch on the CP blade) on the active CP before the heartbeat is up on a power cycle, and the CPs came up non-redundant, reboot the CPs again to clear the problem.

## Severity

WARNING

# FW-1434

## Message

```
timestamp, [FW-1434], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Blade: number-bad blade failures.
```

## Probable cause

The switch status is not in a healthy state because the number of blade failures is greater than or equal to the policy set by the `switchStatusPolicySet` command.

## Recommended action

Replace the faulty blade.

## Severity

WARNING

# FW-1435

## Message

```
timestamp, [FW-1435], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Flash: usage out of range.
```

## Probable cause

The switch status is not in a healthy state because the flash usage is out of range. The policy was set using the `switchStatusPolicySet` command.



## Recommended action

Run the `saveCore` command to clear out the kernel flash. Refer to the *HP StorageWorks Fabric OS 4.x command reference guide* for more information about this command.

## Severity

WARNING

# FW-1436

## Message

```
timestamp, [FW-1436], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Marginal ports: number-of-marginal-ports  
marginal ports.
```

## Probable cause

The switch status is not in a healthy state because the number of marginal ports is greater than or equal to the policy set using the `switchStatusPolicySet` command.

A port is faulty when the port value for Link Loss, Synchronization Loss, Signal Loss, Invalid word, Protocol error, CRC error, Port state change, or Buffer Limited Port is above the high boundary.

## Recommended action

Replace any faulty or deteriorating SFPs.

## Severity

WARNING

# FW-1437

## Message

```
timestamp, [FW-1437], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Faulty ports: number-of-faulty-ports  
faulty ports.
```

## Probable cause

The switch status is not in a healthy state because the number of faulty ports is greater than or equal to the policy set by the `switchStatusPolicySet` command. A port is considered faulty because of a hardware failure, such as a faulty SFP or port.

## Recommended action

Replace any faulty or deteriorating SFPs.

## Severity

WARNING

## FW-1438

### Message

```
timestamp, [FW-1438], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Missing SFPs: number-of-missing-SFPs  
missing SFPs.
```

### Probable cause

The switch status is not in a healthy state because the number of missing SFPs is greater than or equal to the policy set by the `switchStatusPolicySet` command.

### Recommended action

Run the `switchStatusPolicySet` command to modify the SFP policy or to add SFPs to the empty ports.

### Severity

WARNING

## FW-1439

### Message

```
timestamp, [FW-1439], sequence-number,, WARNING, system-name, Switch  
status change contributing factor Switch offline.
```

### Probable cause

The switch status is not in a healthy state because it is offline.

### Recommended action

Run the `switchEnable` command.

### Severity

WARNING

## FW-1440

### Message

```
timestamp, [FW-1440], sequence-number,, INFO, system-name, FRU-label state  
has changed to absent.
```

### Probable cause

The state of the specified FRU changed to absent.

## Recommended action

No action is required. Verify that the event was planned.

## Severity

INFO

# FW-1441

## Message

```
timestamp, [FW-1441], sequence-number,, INFO, system-name, FRU-label state  
has changed to inserted.
```

## Probable cause

The state of the specified FRU changed to `inserted`. This means that a FRU is inserted but not powered on.

## Recommended action

No action is required. Verify that the event was planned.

## Severity

INFO

# FW-1442

## Message

```
timestamp, [FW-1442], sequence-number,, INFO, system-name,  
FRU-label state has changed to on.
```

## Probable cause

The state of the specified FRU changed to `on`.

## Recommended action

No action is required. Verify that the event was planned.

## Severity

INFO

## FW-1443

### Message

```
timestamp, [FW-1443], sequence-number,, INFO, system-name,  
FRU-label state has changed to off.
```

### Probable cause

The state of the specified FRU changed to `off`.

### Recommended action

No action is required. Verify that the event was planned.

### Severity

INFO

## FW-1444

### Message

```
timestamp, [FW-1444], sequence-number,, WARNING, system-name, FRU-label  
state has changed to faulty.
```

### Probable cause

The state of the specified FRU changed to `faulty`.

### Recommended action

Replace the FRU.

### Severity

WARNING

---

## High-availability management error messages

## HAM-1001

### Message

```
timestamp, [HAM-1001], sequence-number,, CRITICAL, system-name, Standby CP  
is not Healthy, device device-name status BAD, severity = severity
```

### Probable cause

A standby CP device error was reported by the high-availability manager (HAM) Health Monitor, with a specific device and severity level. The severity level can be `critical`, `major`, or `minor`.

The active CP continues to function normally, but because the standby CP is not healthy, nondisruptive failover is not possible.

### Recommended action

1. Reboot the standby CP blade by ejecting the card and reseating it.
2. If the problem persists, replace the standby CP.

### Severity

CRITICAL

## HAM-1002

### Message

```
timestamp, [HAM-1002], sequence-number,, INFO, system-name, Standby CP is Healthy
```

### Probable cause

Indicates that all the standby CP devices monitored by the high-availability manager (HAM) Health Monitor report no error.

### Recommended action

No action is required.

### Severity

INFO

## HAM-1004

### Message

```
timestamp, [HAM-1004], sequence-number,, INFO, system-name, reboot-reason
```

### Probable cause

The high-availability manager (HAM) module does not have any information about the reason for switch reboot.

This message records switch reboots that were not initiated by a user or by the `firmwareDownload` command. Some examples of errors that may initiate this message are hardware errors, software errors, compact flash errors, or memory errors. Because the firmware does not know the reason for this reboot, no extra information is displayed.

### Recommended action

Check the error log on both control processors (CPs) for additional messages that may indicate the reason for the reboot.

## Severity

INFO

# HAM-1005

## Message

```
timestamp, [HAM-1005], sequence-number,, CRITICAL, system-name, error-text
```

## Probable cause

The high-availability manager (HAM) has encountered a critical error.

## Recommended action

1. Run the `haDump` command and capture output.
2. Call your switch service provider.

## Severity

CRITICAL

---

# High-availability management kernel module error messages

## HAMK-1001

## Message

```
timestamp, [HAMK-1001], sequence-number,, ERROR, system-name, Error  
notification received: error-information
```

## Probable cause

The high-availability manager kernel (HAMK) has been notified of a problem in the system. The source error itself is logged before this message is logged. Depending on the severity of the message logged, HAM fails over for the Core Switch 2/64 or SAN Director 2/128 and reboots for all other platforms.

## Recommended action

No action is required.

## Severity

ERROR

# HAMK-1002

## Message

```
timestamp, [HAMK-1002], sequence-number,, WARNING, system-name, Heartbeat  
down
```

## Probable cause

The active CP blade determined that the standby CP blade is down. This may occur as a result of an operator-initiated action, such as `firmwareDownload`, if the standby CP blade is reset or removed, or as a result of an error in the standby CP blade.

## Recommended action

1. Monitor the standby CP blade for a few minutes.  
If this message is due to a standby CP reboot, the message HAMK-1003 appears after the standby CP has completed the reboot successfully.
2. If the standby CP does not successfully connect to the active CP after 10 minutes, reboot the standby CP blade by ejecting the blade and reseating it.

## Severity

WARNING

# HAMK-1003

## Message

```
timestamp, [HAMK-1003], sequence-number,, INFO, system-name, Heartbeat up
```

## Probable cause

The active CP blade detects the standby CP blade. The standby CP blade is available to take over in case a failure occurs on the active CP blade. This message is typically seen when the standby CP blade reboots.

## Recommended action

No action is required. This message means that the standby CP is healthy.

## Severity

INFO

---

# Hardware independent layer error messages

## HIL-1101

### Message

```
timestamp, [HIL-1101], sequence-number,, ERROR, system-name, Slot  
slot-number faulted, nominal-voltage (measured-voltage) is above  
threshold.
```

### Probable cause

The blade voltage is above threshold. This message is specific to the Core Switch 2/64 or SAN Director 2/128.

### Recommended action

Replace the faulty blade.

### Severity

ERROR

## HIL-1102

### Message

```
timestamp, [HIL-1102], sequence-number,, ERROR, system-name, Slot  
slot-number faulted, nominal-voltage (measured-voltage) is below  
threshold.
```

### Probable cause

The blade voltage is below threshold. This message is specific to the Core Switch 2/64 or SAN Director 2/128.

### Recommended action

Replace the faulty blade.

### Severity

ERROR

## HIL-1103

### Message

```
timestamp, [HIL-1103], sequence-number,, ERROR, system-name, Blower  
blower-number faulted, nominal-voltage (measured-voltage) is above  
threshold.
```



## Probable cause

The fan voltage is above threshold.

## Recommended action

1. Run the `psShow` command to verify the power supply status.
2. Try to reseat the faulty fan FRU and power supply FRU to verify that they are seated properly.
3. If the problem persists, replace the fan FRU or the power supply FRU as necessary.

## Severity

ERROR

# HIL-1104

## Message

```
timestamp, [HIL-1104], sequence-number,, ERROR, system-name, Blower  
blower-number faulted, nominal-voltage (measured-voltage) is below  
threshold.
```

## Probable cause

The fan voltage is below threshold.

## Recommended action

1. Run the `psShow` command to verify the power supply status.
2. Try to reseat the faulty fan FRU and power supply FRU to verify that they are seated properly.
3. If the problem persists, replace the fan FRU or the power supply FRU as necessary.

## Severity

ERROR

# HIL-1105

## Message

```
timestamp, [HIL-1105], sequence-number,, ERROR, system-name, Switch error,  
nominal-voltage (measured-voltage) above threshold.
```

## Probable cause

The switch voltage is above threshold. This message is specific to non-bladed switches and is not applicable to the Core Switch 2/64 or SAN Director 2/128.

## Recommended action

For the SAN Switch 2/8V and SAN Switch 2/16V, replace the entire switch; these switches do not have FRUs.

For the SAN Switch 2/32, replace the motherboard FRU.

For the SAN Switch 4/32, if the 12-volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

## Severity

ERROR

# HIL-1106

## Message

```
timestamp, [HIL-1106], sequence-number,, ERROR, system-name, Switch error,  
nominal-voltage (measured-voltage) below threshold.
```

## Probable cause

Switch voltage is below threshold. This message is specific to non-bladed switches and is not applicable to the Core Switch 2/64 or SAN Director 2/128.

## Recommended action

For the SAN Switch 2/8V and SAN Switch 2/16V, replace the entire switch; these switches do not have FRUs.

For the SAN Switch 2/32, replace the motherboard FRU.

For the SAN Switch 4/32, if the 12-volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

## Severity

ERROR

# HIL-1107

## Message

```
timestamp, [HIL-1107], sequence-number,, CRITICAL, system-name, Switch  
faulted, nominal-voltage (measured-voltage) above threshold. System  
preparing for reset.
```

## Probable cause

Switch voltage is above threshold. This message is specific to non-bladed switches and is not applicable to the Core Switch 2/64 or SAN Director 2/128.

## Recommended action

For the SAN Switch 2/8V and SAN Switch 2/16V, replace the entire switch; these switches do not have FRUs.

For the SAN Switch 2/32, replace the motherboard FRU.

For the SAN Switch 4/32, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

## Severity

CRITICAL

# HIL-1108

## Message

```
timestamp, [HIL-1108], sequence-number,, CRITICAL, system-name, Switch  
faulted, nominal-voltage (measured-voltage) below threshold. System  
preparing for reset.
```

## Probable cause

Switch voltage is below threshold. This message is specific to non-bladed switches and is not applicable to the Core Switch 2/64 or SAN Director 2/128.

## Recommended action

For the SAN Switch 2/8V and SAN Switch 2/16V, replace the entire switch; these switches do not have FRUs.

For the SAN Switch 2/32, replace the motherboard FRU.

For the SAN Switch 4/32, if the 12 volt level is faulty, replace one or both power supplies. If any other voltage is faulty, replace the entire switch.

## Severity

CRITICAL

# HIL-1201

## Message

```
timestamp, [HIL-1201], sequence-number,, WARNING, system-name, Blower  
blower-number, speed (measured-speed RPM) above threshold.
```

## Probable cause

Fan speed (in RPM) rose above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

## Recommended action

1. Run the `tempShow` command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.
2. Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.
3. Run the `fanShow` command to monitor the speed of the fan generating this error.
4. If the fan continues to generate this message, replace the fan FRU.

## Severity

WARNING

# HIL-1202

## Message

```
timestamp, [HIL-1202], sequence-number,, ERROR, system-name, Blower  
blower-number faulted, speed (measured-speed RPM) below threshold.
```

## Probable cause

The specified fan speed (in RPM) fell below the minimum threshold.

## Recommended action

Replace the fan FRU.

## Severity

ERROR

# HIL-1203

## Message

```
timestamp, [HIL-1203], sequence-number,, ERROR, system-name, Fan  
fan-number faulted, speed (measured-speed RPM) above threshold.
```

## Probable cause

The specified fan speed (in RPM) rose above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

## Recommended action

1. Run the `tempShow` command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.
2. Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.
3. Run the `fanShow` command to monitor the speed of the fan generating this error.
4. If the fan continues to generate this message, replace the fan FRU.

## Severity

ERROR

# HIL-1204

## Message

```
timestamp, [HIL-1204], sequence-number,, ERROR, system-name, Fan  
fan-number faulted, speed (measured-speed RPM) below threshold.
```

## Probable cause

The specified fan speed (in RPM) fell below the minimum threshold. This message is specific to non-bladed switches and is not applicable to the Core Switch 2/64 or SAN Director 2/128.

## Recommended action

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the SAN Switch 2/8V and SAN Switch 2/16V, replace the entire switch; these switches do not have FRUs.

## Severity

ERROR

# HIL-1205

## Message

```
timestamp, [HIL-1205], sequence-number,, ERROR, system-name,  
Fan fan-number sensor sensor-number, speed (measured-speed RPM) above  
threshold.
```

## Probable cause

The specified fan speed (in RPM) rose above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

## Recommended action

1. Run the `tempShow` command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.
2. Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.
3. Run the `fanShow` command to monitor the speed of the fan generating this error.
4. If the fan continues to generate this message, replace the fan FRU.

## Severity

ERROR

# HIL-1206

## Message

```
timestamp, [HIL-1206], sequence-number,, ERROR, system-name,  
Fan fan-number sensor sensor-number, speed (measured-speed RPM) below  
threshold.
```

## Probable cause

The specified fan speed (in RPM) fell below the minimum threshold. This problem can quickly cause the switch to overheat. This message is specific to non-bladed switches and is not applicable to the Core Switch 2/64 or SAN Director 2/128.

## Recommended action

For the SAN Switch 2/32 and SAN Switch 4/32, replace the fan FRU.

For the SAN Switch 2/8V and SAN Switch 2/16V, replace the entire switch; these switches do not have FRUs.

## Severity

ERROR

# HIL-1301

## Message

```
timestamp, [HIL-1301], sequence-number,, ERROR, system-name, 1 blower  
failed. Replace failed blower assembly immediately.
```

## Probable cause

A fan FRU failed. This message is often preceded by a low-speed error message. This problem can quickly cause the switch to overheat.

## Recommended action

Replace the faulty fan FRU immediately.

## Severity

ERROR

# HIL-1302

## Message

```
timestamp, [HIL-1302], sequence-number,, ERROR, system-name,  
count blowers failed. Replace failed blower assemblies immediately.
```

## Probable cause

Multiple fan FRUs failed on a switch. This message is often preceded by a low-fan-speed message.

## Recommended action

Replace the faulty fan FRUs immediately.

## Severity

ERROR

# HIL-1303

## Message

```
timestamp, [HIL-1303], sequence-number,, ERROR, system-name, One fan failed. Replace failed fan FRU immediately.
```

## Probable cause

A fan FRU failed. This message is often preceded by a low-fan-speed message.

## Recommended action

Replace the faulty fan FRU immediately.

## Severity

ERROR

# HIL-1304

## Message

```
timestamp, [HIL-1304], sequence-number,, ERROR, system-name, Two fans failed. Replace failed fan FRUs immediately.
```

## Probable cause

Two fan FRUs failed. This message is often preceded by a low-fan-speed message.

## Recommended action

Replace the faulty fan FRUs immediately.

## Severity

ERROR

# HIL-1305

## Message

```
timestamp, [HIL-1305], sequence-number,, ERROR, system-name, One or two fan(s) failed. Replace failed fan FRU(s) immediately.
```

## Probable cause

One or two fan FRUs failed. This message is often preceded by a low-fan-speed message.

## Recommended action

Replace the faulty fan FRUs immediately.

## Severity

ERROR

# HIL-1306

## Message

```
timestamp, [HIL-1306], sequence-number,, ERROR, system-name, Three fans failed. Replace failed fan FRUs immediately.
```

## Probable cause

Three fan FRUs failed. This message is often preceded by a low-fan-speed message.

## Recommended action

Replace the faulty fan FRUs immediately.

## Severity

ERROR

# HIL-1307

## Message

```
timestamp, [HIL-1307], sequence-number,, ERROR, system-name, Four or five fans failed. Replace failed fan FRUs immediately.
```

## Probable cause

Multiple fan FRUs have . This message is often preceded by a low-fan-speed message.

## Recommended action

Replace the faulty fan FRUs immediately.



## Severity

ERROR

# HIL-1308

## Message

```
timestamp, [HIL-1308], sequence-number,, ERROR, system-name, All fans failed. Replace failed fan FRUs immediately.
```

## Probable cause

All fans failed. This message is often preceded by a low-fan-speed message.

## Recommended action

Replace the faulty fan FRUs immediately.

## Severity

ERROR

# HIL-1309

## Message

```
timestamp, [HIL-1309], sequence-number,, ERROR, system-name, count fan FRU(s) failed. Replace failed fan FRU(s) immediately.
```

## Probable cause

Multiple fans failed. This message is often preceded by a low-fan-speed message.

## Recommended action

Replace the faulty fan FRUs immediately.

## Severity

ERROR

# HIL-1401

## Message

```
timestamp, [HIL-1401], sequence-number,, WARNING, system-name, One fan FRU missing. Install fan FRU immediately.
```

## Probable cause

One fan FRU was removed.

## Recommended action

Install the missing fan FRU.

## Severity

WARNING

# HIL-1402

## Message

```
timestamp, [HIL-1402], sequence-number,, WARNING, system-name, Two fan FRUs missing. Install fan FRUs immediately.
```

## Probable cause

Two fan FRUs were removed.

## Recommended action

Install the missing fan FRUs immediately.

## Severity

WARNING

# HIL-1403

## Message

```
timestamp, [HIL-1403], sequence-number,, WARNING, system-name, All fan FRUs missing. Install fan FRUs immediately.
```

## Probable cause

All fan FRUs were removed.

## Recommended action

Install the missing fan FRUs immediately.

## Severity

WARNING

# HIL-1404

## Message

```
timestamp, [HIL-1404], sequence-number,, WARNING, system-name, count fan FRU(s) missing. Install fan FRU(s) immediately.
```

## Probable cause

One or more fan FRUs were removed.

## Recommended action

Install the missing fan FRUs immediately.

## Severity

WARNING

# HIL-1501

## Message

```
timestamp, [HIL-1501], sequence-number,, WARNING, system-name,  
Slot slot-number, high temperature (measured-temperature).
```

## Probable cause

The temperature of this blade rose above the warning threshold.

## Recommended action

1. Run the `fanShow` command to verify that all fans are operating properly.
2. Make sure that the area is well ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

## Severity

WARNING

# HIL-1502

## Message

```
timestamp, [HIL-1502], sequence-number,, CRITICAL, system-name, Slot  
slot-number, high temperature (measured-temperature). Unit will be shut  
down in 2 minutes if temperature remains high.
```

## Probable cause

The temperature of this blade rose above the critical threshold. This usually follows a high-temperature message.

## Recommended action

1. Run the `fanShow` command to verify all the fans are working properly.
2. Make sure that the area is well ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.
3. If the message persists, replace the blade.

## Severity

CRITICAL

# HIL-1503

## Message

```
timestamp, [HIL-1503], sequence-number,, CRITICAL, system-name, Slot  
slot-number, unit shutting down.
```

## Probable cause

The temperature of this blade kept above the maximum threshold for at least two minutes. The blade is shut down to prevent further damage. This usually follows a high-temperature warning message.

## Recommended action

1. Run the `fanShow` command to verify all the fans are working properly.
2. Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.
3. If the message persists, replace the faulty blade.

## Severity

CRITICAL

# HIL-1504

## Message

```
timestamp, [HIL-1504], sequence-number,, INFO, system-name, System within  
normal temperature specifications (measured-temperature C).
```

## Probable cause

Temperature in the system has returned to normal.

## Recommended action

No action is required.

## Severity

INFO

# HIL-1505

## Message

```
timestamp, [HIL-1505], sequence-number,, WARNING, system-name,  
High temperature (measured-temperature C) exceeds environmental  
specifications.
```

## Probable cause

Temperature in the system rose above the warning threshold.

## Recommended action

1. Run the `fanShow` command to verify all the fans are working properly.
2. Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

## Severity

WARNING

# HIL-1506

## Message

```
timestamp, [HIL-1506], sequence-number,, CRITICAL, system-name, High  
temperature (measured-temperature C) exceeds system temperature limit.  
System will shut down within 2 minutes.
```

## Probable cause

Temperature in the system rose above the critical threshold.

## Recommended action

1. Run the `fanShow` command to verify that all fans are working properly. Replace any deteriorating fan FRUs.
2. Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

## Severity

CRITICAL

# HIL-1507

## Message

```
timestamp, [HIL-1507], sequence-number,, CRITICAL, system-name, High  
temperature warning time expired. System preparing for shutdown.
```

## Probable cause

Temperature in the system rose above the critical threshold.

## Recommended action

Temperatures have probably caused damage to the switch; the system shuts down automatically.

1. To help prevent future problems, make sure that all the fans are working properly.
2. Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

## Severity

CRITICAL

# HIL-1508

## Message

```
timestamp, [HIL-1508], sequence-number,, CRITICAL, system-name, Fan faulty  
warning time expired. System preparing for shutdown.
```

## Probable cause

Temperature in the system remained above the critical threshold too long. Temperature has probably caused damage to the switch; the system shuts down automatically.

## Recommended action

1. To help prevent future problems, make sure that all the fans are working properly.
2. Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

## Severity

CRITICAL

# HIL-1509

## Message

```
timestamp, [HIL-1509], sequence-number,, CRITICAL, system-name, High  
temperature (measured-temperature C). Warning time expired. System  
preparing for shutdown.
```

## Probable cause

Temperature in the system rose above the critical threshold. Temperature has probably caused damage to the switch; the system shuts down automatically.

## Recommended action

1. To help prevent future problems, make sure that all the fans are working properly.
2. Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

## Severity

CRITICAL

# HIL-1601

## Message

```
timestamp, [HIL-1601], sequence-number,, ERROR, system-name, Using backup  
temperature sensor. Service immediately.
```

## Probable cause

Temperature readings from the primary sensor are out of range.

## Recommended action

1. Run the `fanShow` command to verify that all fans are operating correctly.
2. Replace any deteriorating fan FRUs.
3. Run the `tempShow` command to verify temperature values.
4. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

## Severity

ERROR

# HIL-1602

## Message

```
timestamp, [HIL-1602], sequence-number,, CRITICAL, system-name, All  
temperature sensors failed. Service immediately.
```

## Probable cause

Temperature readings from all sensors are out of range.

## Recommended action

1. Run the `fanShow` command to verify that all fans are operating correctly.
2. Replace any deteriorating fan FRUs.
3. Run the `tempShow` command to verify temperature values.
4. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

## Severity

CRITICAL

---

# HELLO protocol error messages

## HLO-1001

## Message

```
timestamp, [HLO-1001], sequence-number,, ERROR, system-name, Incompatible  
Inactivity timeout dead-timeout from port port-number, correct value value
```

## Probable cause

The HLO message is incompatible with the value specified in the FSPF protocol. The switch does not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO dead timeout value is not configurable, so this error can occur only when the HP StorageWorks switch is connected to a switch from another manufacturer.

## Recommended action

The dead timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation of the other manufacturer's switch to change this value.

## Severity

ERROR



# HLO-1002

## Message

```
timestamp, [HLO-1002], sequence-number,, ERROR, system-name, Incompatible  
Hello timeout HLO-timeout from port port-number, correct value  
correct-value
```

## Probable cause

The HLO message is incompatible with the value specified in the FSPF protocol. The switch does not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO timeout value is not configurable, so this error can occur only when the HP StorageWorks switch is connected to a switch from another manufacturer.

## Recommended action

The HLO timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation of the other manufacturer's switch to change this value.

## Severity

ERROR

# HLO-1003

## Message

```
timestamp, [HLO-1003], sequence-number,, ERROR, system-name, Invalid Hello  
received from port port-number, Domain = domain-ID, Remote Port =  
remote-port-ID
```

## Probable cause

The HLO message received is invalid and the frame was dropped. The switch does not accept FSPF frames from the remote switch.

The switch received an invalid HLO because either the domain or port number in the HLO message has an invalid value. This error can occur only when the HP StorageWorks switch is connected to a switch from another manufacturer.

## Recommended action

The HLO message of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation of the other manufacturer's switch to change this value.

## Severity

ERROR

---

# Health monitor error messages

## HMON-1001

### Message

```
timestamp, [HMON-1001], sequence-number,, CRITICAL, system-name,  
failure-description
```

### Probable cause

A problem was encountered reading an essential file containing configuration information from the nonvolatile storage device. This could be the result of a missing file or a corrupt file system.

### Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware to your switch.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

CRITICAL

---

# Hypertext transfer protocol error messages

## HTTP-1001

### Message

```
timestamp, [HTTP-1001], sequence-number,, INFO, system-name, Switch  
PIDformat has changed to current-PID-format.
```

### Probable cause

The PID format has been changed by the administrator.

### Recommended action

No action is required. For more information on PID format, refer to the *HP StorageWorks Fabric OS 4.x procedures user guide*.

### Severity

INFO

---

# Kernel software watchdog error messages

## KSWD-1003

### Message

```
timestamp, [KSWD-1003], sequence-number,, WARNING, system-name, kSWD:  
warning-message
```

### Probable cause

A warning state exists within the system.

### Recommended action

No action is required.

### Severity

WARNING

---

# Kernel RAS trace module error messages

## KTRC-1001

### Message

```
timestamp, [KTRC-1001], sequence-number,, WARNING, system-name, Dump  
memory size exceeds dump file size
```

### Probable cause

The dump memory size exceeds the dump file size.

### Recommended action

No action is required.

### Severity

WARNING

## KTRC-1002

### Message

```
timestamp, [KTRC-1002], sequence-number,, INFO, system-name, Concurrent  
trace dumping.
```

## Probable cause

The initial background dump has not completed.

## Recommended action

No action is required.

## Severity

INFO

# KTRC-1003

## Message

```
timestamp, [KTRC-1003], sequence-number,, ERROR, system-name, Cannot open  
ATA dump device
```

## Probable cause

The ATA dump driver is not initialized properly.

## Recommended action

Properly initialize the ATA dump driver.

## Severity

ERROR

# KTRC-1004

## Message

```
timestamp, [KTRC-1004], sequence-number,, ERROR, system-name, Cannot write  
to ATA dump device
```

## Probable cause

The write boundary in the ATA dump device was exceeded.

## Recommended action

No action is required.

## Severity

ERROR

---

# RASLog subsystem error messages

## LOG-1000

### Message

```
timestamp, [LOG-1000], sequence-number,, INFO, system-name, Previous  
message repeated repeat-count time(s)
```

### Probable cause

The previous message was repeated the number of times specified.

### Recommended action

No action is required.

### Severity

INFO

## LOG-1001

### Message

```
timestamp, [LOG-1001], sequence-number,, CRITICAL, system-name,  
A log message was dropped
```

### Probable cause

A log message was dropped. A trace dump file was created.

### Recommended action

1. Run the `reboot` command for non-bladed switches or the `haFailover` command on bladed switches.
2. Run the `saveCore` command to FTP core files to a server location.
3. Run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

### Severity

CRITICAL

## LOG-1002

### Message

```
timestamp, [LOG-1002], sequence-number,, CRITICAL, system-name,  
A log message was dropped
```

## Probable cause

A message was not recorded by the error logging system. A trace dump file was created. The message may still be visible through SNMP or other management tools.

## Recommended action

1. Run the `reboot` command for non-bladed switches or the `haFailover` command on bladed switches.
2. Run the `saveCore` command to FTP core files to a server location.
3. Run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

## Severity

CRITICAL

---

# Link state database error messages

## LSDB-1001

### Message

```
timestamp, [LSDB-1001], sequence-number,, ERROR, system-name, Link State  
ID link-state-ID out of range
```

## Probable cause

The link state database ID is out of the acceptable range. The valid *link-state-ID* is the same as the valid domain ID, whose range is 1 through 239. The switch discards the record because it is not supported.

## Recommended action

No action is required.

## Severity

ERROR

## LSDB-1002

### Message

```
timestamp, [LSDB-1002], sequence-number,, INFO, system-name, Local Link  
State Record reached max incarnation#
```

## Probable cause

The local link state database reached the maximum incarnation.

An *incarnation* is a progressive number that identifies the most recent version of the link state record (LSR). The switch generates its local LSR when first enabled.

## Recommended action

No action is required. The incarnation count begins again at 1 after reaching 239.

## Severity

INFO

# LSDB-1003

## Message

```
timestamp, [LSDB-1003], sequence-number,, CRITICAL, system-name,  
No database entry for local Link State Record, domain local-domain
```

## Probable cause

No local link state record entry exists in the link state database. The switch should always generate its own local entry when starting up.

An *incarnation* is a progressive number that identifies the most recent version of the link state record (LSR). The switch generates its local link state record when first enabled. By disabling and enabling the switch, a new local LSR is generated.

## Recommended action

Run the `switchDisable` and `switchEnable` commands. A new local LSR is generated during the switch enable.

## Severity

CRITICAL

# LSDB-1004

## Message

```
timestamp, [LSDB-1004], sequence-number,, WARNING, system-name, No Link  
State Record for domain local-domain
```

## Probable cause

No link state record (LSR) exists for the specified *local-domain*.

## Recommended action

No action is required. The other switch passes the LSR when the fabric becomes stable.

## Severity

WARNING

---

# Multicast path error messages

## MPTH-1001

### Message

```
timestamp, [MPTH-1001], sequence-number,, ERROR, system-name, Null parent,  
lsId = number
```

### Probable cause

A null parent was reported. MPATH uses a tree structure in which the parent is used to connect to the root of the tree.

### Recommended action

No action is required.

### Severity

ERROR

## MPTH-1002

### Message

```
timestamp, [MPTH-1002], sequence-number,, ERROR, system-name, Null lsrP,  
lsId = ls-ID-number
```

### Probable cause

A link state record is null.

### Recommended action

No action is required.

### Severity

ERROR

## MPTH-1003

### Message

```
timestamp, [MPTH-1003], sequence-number,, WARNING, system-name,  
No minimum cost path in candidate list
```



## Probable cause

The FSPF module determined that no minimum cost path (MPath) is available in the candidate list.

## Recommended action

No action is required.

## Severity

WARNING

---

# Message queue error messages

## MQ-1004

### Message

```
timestamp, [MQ-1004], sequence-number,, ERROR, system-name, mqRead, queue  
= queue-name, queue ID = queue-ID, type = message-type
```

## Probable cause

An unexpected message was received in the specified message queue. The *queue-name* is always *fspf\_q*. The *queue-ID* and *message-type* can be any of the following:

- 2, MSG\_TX
- 3, MSG\_INTR
- 4, MSG\_STR
- 6, MSG\_ASYNC\_IU
- 7, MSG\_LINIT\_IU
- 8, MSG\_RSCN
- 9, MSG\_IOCTL
- 10, MSG\_ACCEPT
- 11, MSG\_IU\_FREE
- 12, MSG\_US
- 13, MSG\_EXT\_RSCN
- 14, MSG\_RDTS\_START
- 15, MSG\_RDTS\_SENDEFP
- 16, MSG\_RDTS\_RESET

## Recommended action

No action is required.

## Severity

---

# Management service error messages

## MS-1001

### Message

```
timestamp, [MS-1001], sequence-number,, WARNING, system-name, MS Platform  
Segmented port=port-number(reason-for-segmentation domain)
```

### Probable cause

The management server (MS) segmented from another switch *domain* at the specified *port-number* due to errors or inconsistencies defined in the MS platform service.

### Recommended action

Reboot or power cycle the switch.

### Severity

WARNING

## MS-1002

### Message

```
timestamp, [MS-1002], sequence-number,, INFO, system-name, MS Platform  
Service Unstable(message-string domain-number)
```

### Probable cause

The MS platform service is unstable.

The *message-string* can be one of the following:

- No Resp for GCAP from  
The switch did not respond to a request for GCAP (MS Get Capabilities) command.
- GCAP sup but not PL by  
The GCAP (MS Get Capabilities) is supported but the flag for MS platform service is not set.
- GCAP Rejected (reason =BUSY) by  
The GCAP (MS Get Capabilities) is not supported by another switch.
- Reject EXGPLDB from  
The request to the exchange platform database has been rejected. The remote switch may be busy.

The *domain-number* is the target domain that caused error.

### Recommended action

The recommended actions are as follows:

- No Resp for GCAP from  
No action is required.
- GCAP sup but not PL by  
Set the flag for the MS Platform Service.
- GCAP Rejected (reason =BUSY) by  
Run the `firmwareDownload` command to upgrade the firmware level on the switch to a level that supports reliable commit service (RCS). RCS is supported in Fabric OS v2.6, v3.1 and later, and v4.1 and later.
- Reject EXGPLDB from  
Wait a few minutes and try the command again.

## Severity

INFO

# MS-1003

## Message

```
timestamp, [MS-1003], sequence-number, , INFO, system-name, MS detected  
Unstable Fabric(message-string domain-number).
```

## Probable cause

MS detected an unstable fabric; the command or operation may not be successfully completed. This message is often transitory.

The *message-string* can be one of the following:

- DOMAIN\_INVALID for a req from  
The domain is invalid for a request.
- No WWN for  
Unable to acquire the World Wide Name (WWN) for the corresponding domain.

The *domain-number* is the target domain that caused error.

## Recommended action

1. The fabric may be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.
2. Run the `fabricShow` command or the `secFabricShow` command to verify that the number of domains matches the Management Server known domains.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

## Severity

INFO

# MS-1004

## Message

```
timestamp, [MS-1004], sequence-number,, INFO, system-name, MS detected  
ONLY 1 Domain(d=domain-in-local-resource).
```

## Probable cause

MS detected an unstable count of domains in its own local resource.

## Recommended action

This message is often transitory.

1. The fabric may be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.
2. Run the `fabricShow` command or the `secFabricShow` command to verify that the number of domains matches the Management Server known domains.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

## Severity

INFO

# MS-1005

## Message

```
timestamp, [MS-1005], sequence-number,, ERROR, system-name, MS Invalid CT  
Response from d=domain
```

## Probable cause

MS received an invalid common transport (CT) response from switch *domain*. MS expects either a CT accept IU or a reject IU. MS received neither response, which violates the Fibre Channel Generic Services (FS-GS) specification.

## Recommended action

Check the integrity of the FC switch at the specified domain. It is not sending correct MS information as defined by the FC-FS standard.

## Severity

ERROR

# MS-1006

## Message

```
timestamp, [MS-1006], sequence-number,, ERROR, system-name, MS Unexpected  
iu_data_sz=number-of-bytes
```

## Probable cause

MS received IU data of unexpected size. The IU payload and the IU size may be inconsistent with each other or with the command that is currently being processed.

## Recommended action

1. Wait a few minutes and try the operation again.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# MS-1007

## Message

```
timestamp, [MS-1007], sequence-number,, INFO, system-name, MS CT  
cmd=0xCT-command, RCS reason=0xRCS-reason-code(RCS-reason-code-string)
```

## Probable cause

The reliable commit service (RCS) failed in MS. All switches in the fabric must be RCS-capable for RCS to be used in the fabric.

The specified MS *CT-command* for an RCS request failed for the specified *RCS\_reason* and is described in more detail in the *RCS\_reason\_code\_string*.

## Recommended action

1. Run the `rCsInfoShow` command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and later, v4.1 and later.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

INFO

# MS-1008

## Message

```
timestamp, [MS-1008], sequence-number,, ERROR, system-name, MS Failure  
while initializing action
```

## Probable cause

MS failed while initializing the specified *action*.

The following actions may be displayed:

- while writing to `ms_els_q`  
MS is unable to write a message to the MS Extended Link Service Queue.
- while inserting timer to timer list  
MS is unable to add a timer to a resource.

## Recommended action

This message is often transitory.

If the error persists, check the available memory on the switch using `memShow`.

## Severity

ERROR

# MS-1021

## Message

```
timestamp, [MS-1021], sequence-number,, ERROR, system-name,  
MS WARMBOOT failure(FSS_MS_WARMINIT failed. Reason=failure-reason)
```

## Probable cause

The FSS warm recovery failed during WARM INIT phase of a reboot.

## Recommended action

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

---

# Neighboring switch finite state machine error messages

## NBFS-1001

### Message

```
timestamp, [NBFS-1001], sequence-number,, INFO, system-name, Duplicate  
E_Port SCN from port portnumber in state state-change-name  
(state-change-number)
```

### Probable cause

A duplicate E\_Port State Change Number was reported. The neighbor finite state machine (NBFSM) states are as follows:

- 0, Down
- 1, Init
- 2, Database Exchange
- 3, Database Acknowledge Wait
- 4, Database Wait
- 5, Full

### Recommended action

No action is required.

### Severity

INFO

## NBFS-1002

### Message

```
timestamp, [NBFS-1002], sequence-number,, ERROR, system-name, Wrong input:  
state-name to neighbor FSM, state current-state-name, port portnumber
```

### Probable cause

The wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0, Down
- 1, Init
- 2, Database Exchange
- 3, Database Acknowledge Wait

- 4, Database Wait
- 5, Full

If this error occurs repeatedly, it means that the protocol implementation between two connected switches has problems.

## Recommended action

Run the `nbrStateShow` command to check the neighbor state of the port listed in the message. If it is FULL, then this message can safely be ignored. Otherwise, run the `portDisable` and `portEnable` commands to refresh the port.

## Severity

ERROR

# NBFS-1003

## Message

```
timestamp, [NBFS-1003], sequence-number,, WARNING, system-name,
DB_XMIT_SET flag not set in state current-state-name, input state-name,
port portnumber
```

## Probable cause

The database transmit set flag was not set for the specified input state on the specified port. Neighbor finite state machine (NBFSM) states are as follows:

- 0, Down
- 1, Init
- 2, Database Exchange
- 3, Database Acknowledge Wait
- 4, Database Wait
- 5, Full

## Recommended action

No action is required. The Fabric OS automatically recovers from this problem.

## Severity

WARNING



---

# Simple name server module error messages

## NS-1001

### Message

```
timestamp, [NS-1001], sequence-number,, WARNING, system-name, The response  
for request 0xCT-command-code from remote switch 0xDomain-ID is larger  
than the max frame size the remote switch can support!
```

### Probable cause

The response payload exceeds the maximum frame size that the remote switch can handle.

### Recommended action

Run the `firmwareDownload` command to upgrade the remote switch with v4.3 or later, or v3.2 or later, as appropriate for the switch type, so that it can support GMI to handle frame fragmentation and reassembly.

You can also reduce the number of devices connected to the local switch.

### Severity

WARNING

## NS-1002

### Message

```
timestamp, [NS-1002], sequence-number,, WARNING, system-name, Remote  
switch 0xDomain-ID has firmware revision lower than 2.2:  
Firmware-Revision-1st-character Firmware-Revision-2nd-character  
Firmware-Revision-3rd-character Firmware-Revision-4th-character which is  
not supported!
```

### Probable cause

The local switch cannot interact with the remote switch due to incompatible or obsolete firmware.

### Recommended action

Run the `firmwareDownload` command to upgrade the remote switch to the latest level of firmware.

### Severity

WARNING

# NS-1003

## Message

```
timestamp, [NS-1003], sequence-number,, INFO, system-name, Number of local  
devices Current-local-device-count, exceeds the standby can support  
Local-device-count-that-standby-can-support, can't send update.
```

## Probable cause

The name server on the standby CP has lower supported capability than the active CP due to different firmware versions running on the active and standby control processors (CPs). This means that the active and standby CPs are out of sync. Any execution of the `haFailover` or `firmwareDownload` commands is disruptive.

## Recommended action

1. To avoid disruption of traffic in the event of an unplanned failover, schedule a `firmwareDownload` so that the active and standby CPs have the same firmware version.
2. Reduce the local device count to follow the capability of the lowest version of firmware.

## Severity

INFO

# NS-1004

## Message

```
timestamp, [NS-1004], sequence-number,, INFO, system-name, Number of local  
devices Current-local-device-count, exceeds the standby can support  
Local-device-count-that-standby-can-support, can't sync.
```

## Probable cause

The Name Server on the standby CP has lower supported capability than the active CP due to different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the `haFailover` or `firmwareDownload` commands is disruptive.

## Recommended action

1. To avoid disruption of traffic in the event of an unplanned failover, schedule a `firmwareDownload` so that the active and standby CPs have the same firmware version.
2. Reduce the local device count to follow the capability of the lowest version of firmware.

## Severity

INFO

---

# Parity data manager error messages

## PDM-1001

### Message

```
timestamp, [PDM-1001], sequence-number,, WARNING, system-name, Failed to  
parse the pdm config
```

### Probable cause

The PDM process could not parse the configuration file. This may be caused by a missing configuration file during the installation.

### Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

WARNING

## PDM-1002

### Message

```
timestamp, [PDM-1002], sequence-number,, WARNING, system-name, ipcInit  
failed
```

### Probable cause

The PDM process could not initialize the IPC mechanism.

### Recommended action

Run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

### Severity

WARNING

## PDM-1003

### Message

```
timestamp, [PDM-1003], sequence-number,, WARNING, system-name, pdm [-d] -S  
service -s instance
```

## Probable cause

A syntax error occurred when trying to launch the PDM process.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1004

## Message

```
timestamp, [PDM-1004], sequence-number, , WARNING, system-name, Memory  
shortage
```

## Probable cause

The PDM process ran out of memory.

## Recommended action

1. Reboot or power cycle the switch.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1005

## Message

```
timestamp, [PDM-1005], sequence-number, , WARNING, system-name, FSS  
register failed
```

## Probable cause

The PDM failed to register to the FSS.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1006

## Message

```
timestamp, [PDM-1006], sequence-number,, WARNING, system-name, Too many  
files in sync.conf
```

## Probable cause

The configuration file `sync.conf` contains too many entries.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1007

## Message

```
timestamp, [PDM-1007], sequence-number,, WARNING, system-name, File not  
created: file-name
```

## Probable cause

The PDM process failed to create the specified file name.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1008

## Message

```
timestamp, [PDM-1008], sequence-number,, WARNING, system-name, Failed to  
get the number of uports
```

## Probable cause

The PDM system call to `getcfg` failed.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1009

## Message

```
timestamp, [PDM-1009], sequence-number,, WARNING, system-name, Can't  
update Port Config Data
```

## Probable cause

The PDM system call to `setcfg` failed.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1010

## Message

```
timestamp, [PDM-1010], sequence-number,, WARNING, system-name, File open  
failed: file-name
```

## Probable cause

The PDM process could not open the specified file name.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1011

## Message

```
timestamp, [PDM-1011], sequence-number,, WARNING, system-name, File read  
failed: file-name
```

## Probable cause

The PDM process could not read data from the specified file name.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1012

## Message

```
timestamp, [PDM-1012], sequence-number,, WARNING, system-name, File write  
failed: file-name
```

## Probable cause

The PDM process could not write data to the specified file name.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1013

## Message

```
timestamp, [PDM-1013], sequence-number,, WARNING, system-name, File empty:  
file-name
```

## Probable cause

The switch configuration file `/etc/fabos/fabos.[0|1].conf` is empty.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1014

## Message

```
timestamp, [PDM-1014], sequence-number,, WARNING, system-name, Access  
sysmod failed
```

## Probable cause

A system call failed.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1017

## Message

```
timestamp, [PDM-1017], sequence-number,, CRITICAL, system-name, System  
(error-code) : command
```

## Probable cause

A system call failed.



## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

CRITICAL

# PDM-1019

## Message

```
timestamp, [PDM-1019], sequence-number,, WARNING, system-name, File path  
or trigger too long
```

## Probable cause

One line of the `pdm.conf` file is too long.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# PDM-1020

## Message

```
timestamp, [PDM-1020], sequence-number,, WARNING, system-name, Long path  
name (path/file-name), Skip
```

## Probable cause

The indicated file path name is too long. The limit is 49 characters.

## Recommended action

Use short path name for the files to be replicated.

## Severity

WARNING

# PDM-1021

## Message

```
timestamp, [PDM-1021], sequence-number,, WARNING, system-name, Failed to  
download area port map
```

## Probable cause

A system call failed.

## Recommended action

1. Run the `firmwareDownload` command to reinstall the firmware.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

---

# Panic dump trace error messages

## PDTR-1001

## Message

```
timestamp, [PDTR-1001], sequence-number,, INFO, system-name, informational  
message
```

## Probable cause

Information was written to the panic dump files. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

## Recommended action

Run the `pdShow` command to view the panic dump and core dump files.

## Severity

INFO

# PDTR-1002

## Message

```
timestamp, [PDTR-1002], sequence-number,, INFO, system-name, informational  
message
```

## Probable cause

Information was written to the panic dump and core dump files and a trap was generated. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

## Recommended action

Run the `pdShow` command to view the panic dump and core dump files.

## Severity

INFO

---

# PLAT error messages

## PLAT-1000

## Message

```
timestamp, [PLAT-1000], sequence-number,, CRITICAL, system-name,  
function-name error-string
```

## Probable cause

Non-recoverable PCI errors were detected.

## Recommended action

The system is faulted and may reboot.

1. If the system does not reboot, try issuing a `reboot` command from a command-line prompt.
2. Run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

CRITICAL

---

# Port error messages

## PORT-1003

### Message

```
timestamp, [PORT-1003], sequence-number,, WARNING, system-name, Port  
port-number Faulted because of many Link Failures
```

### Probable cause

The specified port is now disabled because the link on this port had multiple failures that exceed an internally set threshold on the port. This problem is typically related to hardware.

### Recommended action

1. Check and, if necessary, replace the hardware attached to both ends of the specified *port-number*, including:
  - Media (SFPs)
  - Cable (fiber optic or copper ISL)
  - Attached devices
2. When finished checking the hardware, perform `portEnable` to reenabte the port.

### Severity

WARNING

## PORT-1004

### Message

```
timestamp, [PORT-1004], sequence-number,, INFO, system-name, Port  
port-number could not be enabled because it is disabled due to long  
distance.
```

### Probable cause

The specified port could not be enabled because other ports in the same port group have used up the buffers available for this port group. This occurs when other ports are configured to be long distance.

### Recommended action

To enable this port, reconfigure the other E\_Ports so they are not long distance or change the other E\_Ports so they are not E\_Ports. This frees some buffers and allows this port to be enabled.

### Severity

INFO

---

# Performance server error messages

## PS-1000

### Message

```
timestamp, [PS-1000], sequence-number,, CRITICAL, system-name, Failed to initialize Advanced Performance Monitoring.
```

### Probable cause

An unexpected software error occurred in Advanced Performance Monitoring. The Performance Monitor failed to initialize.

### Recommended action

The control processor (CP) should reboot or fail over automatically. If it does not, reboot or power cycle the switch to reinitiate the firmware.

### Severity

CRITICAL

## PS-1001

### Message

```
timestamp, [PS-1001], sequence-number,, INFO, system-name, Advanced Performance Monitoring configuration updated due to change in PID format
```

### Probable cause

The PID format changed.

### Recommended action

No action is required. Refer to the *HP StorageWorks Fabric OS 4.x procedures user guide* for more information about the PID format.

### Severity

INFO

## PS-1002

### Message

```
timestamp, [PS-1002], sequence-number,, ERROR, system-name, Failed to initialize the tracing system for Advanced Performance Monitoring.
```

## Probable cause

An unexpected software error occurred in Advanced Performance Monitoring. The Performance Monitor tracing system failed to initialize.

## Recommended action

Tracing is be available for Advanced Performance Monitoring, but other functions should perform normally. To reactivate tracing, reboot or fail over the CP.

## Severity

ERROR

# PS-1003

## Message

```
timestamp, [PS-1003], sequence-number,, WARNING, system-name, Failed to  
set end-to-end monitoring mask on ISL ports.
```

## Probable cause

The restoring configuration attempted to set the end-to-end monitoring mask on at least one ISL port.

## Recommended action

No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can be disabled only through the Fabric Access API.

## Severity

WARNING

# PS-1004

## Message

```
timestamp, [PS-1004], sequence-number,, WARNING, system-name, Failed to  
add end-to-end monitors on ISL ports.
```

## Probable cause

The restoring configuration attempted to add end-to-end monitors on at least one ISL port.

## Recommended action

No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can be disabled only through the Fabric Access API.

## Severity

WARNING

# PS-1005

## Message

```
timestamp, [PS-1005], sequence-number,, WARNING, system-name, ISL monitor  
on port port stopped counting because no hardware resources are available
```

## Probable cause

ISL and end-to-end monitors used all the hardware resources.

## Recommended action

To resume counting, delete some end-to-end monitors sharing the same hardware resource pool.

## Severity

WARNING

---

# Portswap feature error messages

## PSWP-1001

## Message

```
timestamp, [PSWP-1001], sequence-number,, INFO, system-name, Areas for  
port wwn-name-corresponding-to-source-port and port  
wwn-name-corresponding-to-destination-port are swapped. New area for port  
wwn-name-corresponding-to-source-port is  
wwn name-corresponding-to-destination-port and port  
new-area-corresponding-to-source-wwn is  
new-area-corresponding-to-destination-wwn
```

## Probable cause

The portSwap command was issued by the user.

## Recommended action

No action is required.

## Severity

INFO

## PSWP-1002

## Message

```
timestamp, [PSWP-1002], sequence-number,, INFO, system-name, Port Swap  
feature enabled
```

## Probable cause

The portSwap feature was enabled in the switch by the user.

## Recommended action

No action is required.

## Severity

INFO

# PSWP-1003

## Message

```
timestamp, [PSWP-1003], sequence-number,, INFO, system-name,  
Port Swap feature disabled
```

## Probable cause

The portSwap feature was disabled in the switch by the user.

## Recommended action

No action is required.

## Severity

INFO

# PSWP-1004

## Message

```
timestamp, [PSWP-1004], sequence-number,, WARNING, system-name, Port Swap  
configuration does not match Chassis configuration for switch  
switch-number. Erasing port swap tables...
```

## Probable cause

The portSwap configuration contradicts the chassis configuration.

## Recommended action

Redefine the port swap configuration to match the chassis configuration.

## Severity

WARNING



---

# Reliable commit service error messages

## RCS-1001

### Message

```
timestamp, [RCS-1001], sequence-number,, INFO, system-name, RCS has been disabled. Some switches in the fabric do not support this feature
```

### Probable cause

The RCS feature was disabled on the local switch because not all switches in the fabric support RCS or the switch is in nonnative mode.

### Recommended action

1. Run the `rcsInfoShow` command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and later, v4.1 and later.
2. Run the `firmwareDownload` command to upgrade the firmware for any switches that do not support RCS.

### Severity

INFO

## RCS-1002

### Message

```
timestamp, [RCS-1002], sequence-number,, INFO, system-name, RCS has been enabled.
```

### Probable cause

The RCS feature was enabled. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

### Recommended action

No action is required.

### Severity

INFO

## RCS-1003

### Message

```
timestamp, [RCS-1003], sequence-number,, ERROR, system-name, Failed to allocate memory: (function-name)
```

## Probable cause

The specified RCS function failed to allocate memory.

## Recommended action

1. This message is usually transitory. Wait a few minutes and retry the command.
2. Check memory usage on the switch using the `memShow` command.
3. Reboot or power cycle the switch.

## Severity

ERROR

# RCS-1004

## Message

```
timestamp, [RCS-1004], sequence-number,, ERROR, system-name,  
Application(application-name) not registered.(error-string)
```

## Probable cause

The specified application did not register with RCS.

## Recommended action

1. Run the `haShow` command to view the HA state.
2. Run the `haDisable` and the `haEnable` commands.
3. Run the `rcsInfoShow` command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and later, v4.1 and later.
4. Run the `firmwareDownload` command to upgrade the firmware for any switches that do not support RCS.

## Severity

ERROR

# RCS-1005

## Message

```
timestamp, [RCS-1005], sequence-number,, INFO, system-name,  
State RCS-phase, Application application-ID returned 0xreject-code.
```

## Probable cause

A receiving switch is rejecting an RCS phase.

## Recommended action

1. If the reject is in ACA phase, wait several minutes and then retry the operation from the sender switch.

2. If the reject is in the SFC phase, check whether the application license exists for the local domain and whether the application data is compatible.

## Severity

INFO

# RCS-1006

## Message

```
timestamp, [RCS-1006], sequence-number,, INFO, system-name, State  
RCS-phase, Application application-ID, RCS CM. Domain  
domain-ID-that-sent-the-reject returned 0xreject-code.
```

## Probable cause

A remote domain rejected an RCS phase initiated by an application on the local switch.

- If the reject phase is ACA, the remote domain may be busy and could not process the new request.
- If the reject phase is SFC, the data sent by the application may not be compatible or the domain does not have the license to support that application.

## Recommended action

1. If the reject is in ACA phase, wait several minutes and then retry the operation.
2. If the reject is in the SFC phase, check whether the application license exists for the remote domain and whether the application data is compatible.

## Severity

INFO

---

# Remote procedure call error messages

# RPCD-1001

## Message

```
timestamp, [RPCD-1001], sequence-number,, WARNING, system-name,  
Authentication Error: client \"IP-address\" has bad credentials:  
bad-user-name-and-password-pair
```

## Probable cause

An authentication error was reported. The specified client *IP-address* has faulty credentials.

## Recommended action

Enter the correct user name and password from the Fabric Access API host.

## Severity

WARNING

# RPCD-1002

## Message

```
timestamp, [RPCD-1002], sequence-number,, WARNING, system-name, Missing  
certificate file. Secure RPCd is disabled.
```

## Probable cause

An SSL certificate is missing.

## Recommended action

To enable RPCD in secure mode, install a valid SSL certificate for the switch.

## Severity

WARNING

# RPCD-1003

## Message

```
timestamp, [RPCD-1003], sequence-number,, WARNING, system-name, Permission  
denied accessing certificate file. Secure RPCd is disabled.
```

## Probable cause

The SSL certificate file configured on the switch cannot be accessed because root does not have read access.

## Recommended action

Change the file system access level for the certificate file to have root read-level access.

## Severity

WARNING

# RPCD-1004

## Message

```
timestamp, [RPCD-1004], sequence-number,, WARNING, system-name, Invalid  
certificate file. Secure RPCd is disabled.
```

## Probable cause

The SSL certificate file is corrupted.

## Recommended action

To enable RPCD in secure mode, install a valid SSL certificate on the switch.

## Severity

WARNING

# RPCD-1005

## Message

```
timestamp, [RPCD-1005], sequence-number,, WARNING, system-name, Missing  
private key file. Secure RPCd is disabled.
```

## Probable cause

The private key file is missing.

## Recommended action

Run the `pkiCreate` command to install a valid private key file.

## Severity

WARNING

# RPCD-1006

## Message

```
timestamp, [RPCD-1006], sequence-number,, WARNING, system-name, Permission  
denied accessing private key file. Secure RPCd is disabled.
```

## Probable cause

The private key file configured on the switch cannot be accessed because root does not have read access.

## Recommended action

Change the file system access level for the private key file to have root read-level access.

## Severity

WARNING

# RPCD-1007

## Message

```
timestamp, [RPCD-1007], sequence-number,, WARNING, system-name, Invalid  
private file. Secure RPCd is disabled.
```

## Probable cause

The private key file is corrupted.

## Recommended action

Run the `pkiCreate` command to install a valid private key file.

## Severity

WARNING

---

# Reliable transport write and read error messages

## RTWR-1001

## Message

```
timestamp, [RTWR-1001], sequence-number,, ERROR, system-name, RTWR  
routine:-error-message 0xdetail1, 0xdetail2, 0xdetail3, 0xdetail4,  
0xdetail5
```

## Probable cause

An error occurred in the RTWR. The message provides the name of the routine having the error and more specific error information. The values in details 1 through 5 provide additional information.

## Recommended action

No action is required.

## Severity

ERROR

## RTWR-1002

## Message

```
timestamp, [RTWR-1002], sequence-number,, WARNING, system-name, RTWR  
error-message 0xdetail1, 0xdetail2, 0xdetail3, 0xdetail4, 0xdetail5
```

## Probable cause

The RTWR exhausted the maximum number of retries sending data to the specified domain. Details are as follows:

- *RTWR error message*: Max retries exhausted
- *detail1*: Port
- *detail2*: Domain
- *detail3*: Retry Count
- *detail4*: Status
- *detail5*: Process ID

## Recommended action

1. Run the `fabricShow` command to see if the specified domain ID is online.
2. Enable the switch with the specified domain ID.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

---

# State change notification error messages

## SCN-1001

### Message

```
timestamp, [SCN-1001], sequence-number,, CRITICAL, system-name, SCN queue  
overflow for process daemon-name
```

## Probable cause

An attempt to write a state change notification (SCN) message to a specific queue failed because the SCN queue for the specified *daemon-name* is full. This may be caused by the daemon hanging or if the system being busy.

Values for *daemon-name* are:

- `fabricd`
- `asd`
- `evmd`
- `fcpd`
- `webd`
- `msd`

- nsd
- psd
- snmpd
- zoned
- fspf
- tsd

## Recommended action

If the message is caused by the system being busy, the condition is temporary.

1. If the message is caused by a hung daemon, the software watchdog causes the daemon to dump the core and reboot the switch. In this case, run the `saveCore` command to send the core files using FTP to a secure server location.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

CRITICAL

# Security error messages

## SEC-1001

### Message

```
timestamp, [SEC-1001], sequence-number,, ERROR, system-name, RCS process
fails: reason-text
```

### Probable cause

The reliable commit service (RCS) process failed to complete.

RCS is a reliable mechanism to transfer data from one switch to other switches within the fabric. This mechanism guarantees that either all switches commit to the new database or none of them update to the new database. This process can fail if one switch in the fabric is busy or in an error state that cannot accept the database.

## Recommended action

1. If the switch is busy, the command may fail the first time only; retry after the first fail. RCS is used when the security database is changed by a command run by security (for example, `secPolicySave`, `secPolicyActivate`, or `secVersionReset`).
2. Run the `rcsInfoShow` command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.



## Severity

ERROR

# SEC-1002

## Message

```
timestamp, [SEC-1002], sequence-number,, ERROR, system-name, Security data  
fails: reason-text
```

## Probable cause

The receiving switch failed to validate the security database sent from the primary FCS switch.

This can result from the data package being corrupted, the time stamp on the package being out of range (as a result of replay attack or out-of-sync time service), or the signature verification having failed. Signature verification failure may be due to an internal error, such as losing the primary public key or an invalid database. If a switch is in the error state, the database may not be correctly updated for that switch.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. The error may also be a result of an internal corruption or a hacker attack to the secure fabric.

## Severity

ERROR

# SEC-1003

## Message

```
timestamp, [SEC-1003], sequence-number,, WARNING, system-name, Fail to  
download security data to domain domain-number after number-of-retries  
retries
```

## Probable cause

The specified domain number failed to download security data after the specified number of attempts. The primary switch segmented the failed switch after 30 tries. The failed switch may have had some internal error, which caused it to fail to accept the database download.

## Recommended action

1. Reset the version stamp on the switch to 0 and then rejoin the switch to the fabric.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

## SEC-1005

### Message

```
timestamp, [SEC-1005], sequence-number,, INFO, system-name, Primary FCS  
receives data request from domain domain-number
```

### Probable cause

The primary FCS received a data request from the specified domain.

For example, if the switch fails to update the database or is attacked (data injection), a message is generated to the primary FCS to try to correct and resync with the rest of the switches in the fabric.

### Recommended action

Check the fabric status, using `secFabricShow` to verify that the fabric is not being attacked by unauthorized users.

### Severity

INFO

## SEC-1006

### Message

```
timestamp, [SEC-1006], sequence-number,, WARNING, system-name, Security  
statistics error: Failed to reset due to invalid data.
```

### Probable cause

Invalid data was received for any statistic-related command for security (`secStatsShow` or `secStatsReset`).

The counter is updated automatically when a security violation occurs. This message may also occur if the updating counter fails.

### Recommended action

1. If the message is the result of a user command, retry the statistic command.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

WARNING

## SEC-1007

### Message

```
timestamp, [SEC-1007], sequence-number,, INFO, system-name, Security  
violation: Unauthorized host with IP address  
IP-address-of-the-violating-host tries to establish API connection.
```

### Probable cause

A security violation was reported. The IP address of the unauthorized host is displayed in the message.

### Recommended action

Check for unauthorized access to the switch through the API connection.

### Severity

INFO

## SEC-1008

### Message

```
timestamp, [SEC-1008], sequence-number,, INFO, system-name, Security  
violation: Unauthorized host with IP address  
IP-address-of-the-violating-host tries to establish HTTP connection.
```

### Probable cause

A security violation was reported. The IP address of the unauthorized host is displayed in the message.

### Recommended action

Check for unauthorized access to the switch through the HTTP connection.

### Severity

INFO

## SEC-1009

### Message

```
timestamp, [SEC-1009], sequence-number,, INFO, system-name, Security  
violation: Unauthorized host with IP address  
IP-address-of-the-violating-host tries to establish TELNET connection.
```

### Probable cause

A security violation was reported. The IP address of the unauthorized host is displayed in the message.

## Recommended action

Check for unauthorized access to the switch through the telnet connection.

## Severity

INFO

# SEC-1016

## Message

```
timestamp, [SEC-1016], sequence-number,, INFO, system-name, Security  
violation: Unauthorized host with IP address  
IP-address-of-the-violating-host tries to establish SSH connection.
```

## Probable cause

A security violation was reported. The IP address of the unauthorized host is displayed in the message.

## Recommended action

Check for unauthorized access to the switch through the SSH connection.

## Severity

INFO

# SEC-1022

## Message

```
timestamp, [SEC-1022], sequence-number,, WARNING, system-name, Failed to  
operation PKI objects.
```

## Probable cause

The security server failed to generate or validate either the public or private key pair or the CSR.

## Recommended action

1. Run the `pkiShow` command and verify that all PKI objects exist on the switch.
2. If the private key does not exist, follow the steps for re-creating PKI objects, outlined in the *HP StorageWorks Secure Fabric OS user guide*.
3. If a certificate does not exist or is invalid, install the certificate by following the field upgrade process.

## Severity

WARNING

## SEC-1024

### Message

```
timestamp, [SEC-1024], sequence-number,, INFO, system-name, The DB-name  
security database is too large to fit in flash.
```

### Probable cause

The size of the security database is too large for the flash memory. The size of the security database increases with the number of entries in each policy.

### Recommended action

Reduce the size of the security database by reducing the number of entries within each policy.

### Severity

INFO

## SEC-1025

### Message

```
timestamp, [SEC-1025], sequence-number,, ERROR, system-name, Invalid IP  
IP-address.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1026

### Message

```
timestamp, [SEC-1026], sequence-number,, ERROR, system-name, Not a valid  
format [switch-member-ID] for switch member.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1028

## Message

```
timestamp, [SEC-1028], sequence-number,, ERROR, system-name, No name is specified.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1029

## Message

```
timestamp, [SEC-1029], sequence-number,, ERROR, system-name, Invalid character in policy-name.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1030

## Message

```
timestamp, [SEC-1030], sequence-number,, ERROR, system-name, The length of  
the name invalid.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1031

## Message

```
timestamp, [SEC-1031], sequence-number,, WARNING, system-name, Current  
security policy DB cannot be supported by standby. CPs will go out of  
sync.
```

## Probable cause

The security database size is not supported by the standby CP.

## Recommended action

Reduce the database size by reducing the security policy size.

## Severity

WARNING

## SEC-1032

### Message

```
timestamp, [SEC-1032], sequence-number,, ERROR, system-name, Empty FCS  
list is not allowed.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1033

### Message

```
timestamp, [SEC-1033], sequence-number,, ERROR, system-name, The * symbol  
is only used to create the policy. Command terminated
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1034

### Message

```
timestamp, [SEC-1034], sequence-number,, ERROR, system-name, Invalid  
member policy-member.
```



## Probable cause

The input list has an invalid member.

## Recommended action

Verify your member names and then input the correct information.

## Severity

ERROR

# SEC-1035

## Message

```
timestamp, [SEC-1035], sequence-number,, ERROR, system-name, Invalid  
device WWN device-WWN.
```

## Probable cause

The specified WWN is invalid.

## Recommended action

Enter the correct WWN value.

## Severity

ERROR

# SEC-1036

## Message

```
timestamp, [SEC-1036], sequence-number,, ERROR, system-name, Invalid  
device name device-name. Missing colon
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1037

## Message

```
timestamp, [SEC-1037], sequence-number,, ERROR, system-name, Invalid WWN  
format invalid-wwn.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1038

## Message

```
timestamp, [SEC-1038], sequence-number,, ERROR, system-name, Invalid  
domain domain-ID.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

## SEC-1040

### Message

```
timestamp, [SEC-1040], sequence-number,, ERROR, system-name, Invalid  
portlist (port-list). Cannot combine * with port member in the same  
portlist.
```

### Probable cause

The port list contains the wildcard asterisk (\*) character.

### Recommended action

You cannot use the asterisk in a port list. Enter the port list values without wildcards.

### Severity

ERROR

## SEC-1041

### Message

```
timestamp, [SEC-1041], sequence-number,, ERROR, system-name, Invalid port  
member port-member in portlist (port-list). reason.
```

### Probable cause

The port member is invalid for one of the following reasons:

- The value is not a number.
- The value is too long. Valid numbers must be between one and three characters long.
- The value cannot be parsed due to invalid characters.

### Recommended action

Use valid syntax when entering port members.

### Severity

ERROR

## SEC-1042

### Message

```
timestamp, [SEC-1042], sequence-number,, ERROR, system-name, Invalid area  
member port-member in portlist (port-list). Out of range (minimum-value -  
maximum-value).
```

## Probable cause

The specified area member is not within the minimum and maximum values.

## Recommended action

Use valid syntax when entering area numbers.

## Severity

ERROR

# SEC-1043

## Message

```
timestamp, [SEC-1043], sequence-number,, ERROR, system-name, Invalid port  
range range-minimum - range-maximum.
```

## Probable cause

The specified port is not within the minimum and maximum range.

## Recommended action

Use valid syntax when entering port ranges.

## Severity

ERROR

# SEC-1044

## Message

```
timestamp, [SEC-1044], sequence-number,, ERROR, system-name, Duplicate  
member member-ID in (list).
```

## Probable cause

The specified member is a duplicate in the input list. The list can be a policy list or a switch member list.

## Recommended action

Do not specify duplicates.

## Severity

ERROR

## SEC-1045

### Message

```
timestamp, [SEC-1045], sequence-number,, ERROR, system-name, Too many port members.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1046

### Message

```
timestamp, [SEC-1046], sequence-number,, ERROR, system-name, Empty list.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1049

### Message

```
timestamp, [SEC-1049], sequence-number,, ERROR, system-name, Invalid switch name switch-name.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1050

## Message

```
timestamp, [SEC-1050], sequence-number,, ERROR, system-name, There are  
more than one switches with the same name switch-name in the fabric.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1051

## Message

```
timestamp, [SEC-1051], sequence-number,, ERROR, system-name, Missing brace  
for port list port-list.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1052

## Message

```
timestamp, [SEC-1052], sequence-number,, ERROR, system-name, Invalid  
input.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1053

## Message

```
timestamp, [SEC-1053], sequence-number,, ERROR, system-name, Invalid pFCS  
list pFCS-list
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1054

## Message

```
timestamp, [SEC-1054], sequence-number,, ERROR, system-name, Invalid FCS  
list length list-length
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1055

## Message

```
timestamp, [SEC-1055], sequence-number,, ERROR, system-name, Invalid FCS  
list WWN-list
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR



## SEC-1056

### Message

```
timestamp, [SEC-1056], sequence-number,, ERROR, system-name, Invalid  
position new-position. Only number-of-members-in-FCS-list members in list.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1057

### Message

```
timestamp, [SEC-1057], sequence-number,, ERROR, system-name, No change.  
Both positions are the same.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1059

### Message

```
timestamp, [SEC-1059], sequence-number,, ERROR, system-name, Fail to  
operation named-item to flash.
```

## Probable cause

The operation failed when writing to flash.

## Recommended action

Run the `saveCore` command to move files off the kernel flash.

## Severity

ERROR

# SEC-1062

## Message

```
timestamp, [SEC-1062], sequence-number,, ERROR, system-name, Invalid  
number of Domains in Domain List.
```

## Probable cause

Either no domains are specified or domains greater than the maximum are specified.

## Recommended action

Enter the correct number of domains.

## Severity

ERROR

# SEC-1063

## Message

```
timestamp, [SEC-1063], sequence-number,, ERROR, system-name, Failed  
to reset statistics.
```

## Probable cause

Either the type or the domains specified are invalid.

## Recommended action

Enter valid data.

## Severity

ERROR

## SEC-1064

### Message

```
timestamp, [SEC-1064], sequence-number,, ERROR, system-name, Failed to  
sign message.
```

### Probable cause

The PKI objects on the switch are not in a valid state and the signature operation failed.

### Recommended action

Run the `pkiShow` command to verify that all PKI objects are valid. If PKI objects are not valid, generate the PKI objects and install the certificate by following the field upgrade process.

### Severity

ERROR

## SEC-1065

### Message

```
timestamp, [SEC-1065], sequence-number,, ERROR, system-name, Invalid  
character in list.
```

### Probable cause

The input list has an invalid character.

### Recommended action

Enter valid data.

### Severity

ERROR

## SEC-1069

### Message

```
timestamp, [SEC-1069], sequence-number,, ERROR, system-name, Security  
Database is corrupted.
```

### Probable cause

The security database is corrupted for unknown reasons.

### Recommended action

Run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# SEC-1071

## Message

```
timestamp, [SEC-1071], sequence-number,, ERROR, system-name, No new data  
to apply.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1072

## Message

```
timestamp, [SEC-1072], sequence-number,, ERROR, system-name, policy-type  
Policy List is Empty!
```

## Probable cause

The specific policy type is empty. The security database is corrupted for unknown reasons.

## Recommended action

Run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

## SEC-1073

### Message

```
timestamp, [SEC-1073], sequence-number,, ERROR, system-name, No FCS policy in list!
```

### Probable cause

The specific policy type is empty. The security database is corrupted for unknown reasons.

### Recommended action

Run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

### Severity

ERROR

## SEC-1074

### Message

```
timestamp, [SEC-1074], sequence-number,, ERROR, system-name, Cannot execute the command on this switch. Please check the secure mode and FCS status.
```

### Probable cause

A security command was run on a switch that is not allowed to run it either because it is in non-secure mode or because it does not have required FCS privilege.

### Recommended action

If a security operation that is not allowed in non-secure mode is attempted, do not perform the operation in non-secure mode. In secure mode, run the command from a switch that has required privilege; that is, either a backup FCS or primary FCS.

### Severity

ERROR

## SEC-1075

### Message

```
timestamp, [SEC-1075], sequence-number,, ERROR, system-name, Fail to operation new policy set on all switches.
```

### Probable cause

A corruption during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1076

## Message

```
timestamp, [SEC-1076], sequence-number,, ERROR, system-name,  
NoNodeWWNZoning option has been changed.
```

## Probable cause

The NoNodeWWNZoning option was changed. If the option is turned on, a zone member can be added using node WWNs, but the member cannot communicate with others nodes in the zone.

## Recommended action

Reenable the current zone configuration for the change to take effect.

## Severity

ERROR

# SEC-1077

## Message

```
timestamp, [SEC-1077], sequence-number,, ERROR, system-name, Failed to  
activate new policy set on all switches.
```

## Probable cause

The policy could not be activated. Reasons can be no memory, switch busy, and so on.

## Recommended action

Run the `secFabricShow` command to verify that all switches in the fabric are in the ready state. Retry the command when all switches are ready.

## Severity

ERROR

## SEC-1078

### Message

```
timestamp, [SEC-1078], sequence-number,, ERROR, system-name, No new data  
to abort.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1079

### Message

```
timestamp, [SEC-1079], sequence-number,, ERROR, system-name, Invalid  
policy name policy-name.
```

### Probable cause

A corruption during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1080

### Message

```
timestamp, [SEC-1080], sequence-number,, ERROR, system-name, Operation  
denied. Please, use secModeEnable command.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1081

## Message

```
timestamp, [SEC-1081], sequence-number,, ERROR, system-name, DCC_POLICY is  
not allowed without a unique identifier.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1082

## Message

```
timestamp, [SEC-1082], sequence-number,, ERROR, system-name, Failed to  
create policy-name policy.
```

## Probable cause

The security policy was not created due to faulty input or low resources.

## Recommended action

Use proper syntax when creating policies. If the security database is too large, you must delete other members within the database before adding new members to a policy.



## Severity

ERROR

# SEC-1083

## Message

```
timestamp, [SEC-1083], sequence-number,, ERROR, system-name, Name already exists.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1084

## Message

```
timestamp, [SEC-1084], sequence-number,, ERROR, system-name, Name exists for different type policy-name.
```

## Probable cause

The specified policy already exists.

## Recommended action

No action is required.

## Severity

ERROR

## SEC-1085

### Message

```
timestamp, [SEC-1085], sequence-number,, ERROR, system-name, Failed to  
create policy-name.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1086

### Message

```
timestamp, [SEC-1086], sequence-number,, ERROR, system-name, The security  
database is too large to fit in flash.
```

### Probable cause

The security database has more data than the flash can accommodate.

### Recommended action

Reduce the number of entries in some policies to decrease the security database size.

### Severity

ERROR

## SEC-1088

### Message

```
timestamp, [SEC-1088], sequence-number,, ERROR, system-name, Cannot  
execute the command. Please try later.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1089

## Message

```
timestamp, [SEC-1089], sequence-number,, ERROR, system-name, Policy name  
policy-name not found. Please, use secPolicyCreate.
```

## Probable cause

There was a corruption during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1090

## Message

```
timestamp, [SEC-1090], sequence-number,, ERROR, system-name, SCC list  
contains FCS member. Please remove member from the FCS policy first.
```

## Probable cause

There was a corruption during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1091

## Message

```
timestamp, [SEC-1091], sequence-number,, ERROR, system-name, No policy to  
remove.
```

## Probable cause

There was a corruption during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1092

## Message

```
timestamp, [SEC-1092], sequence-number,, ERROR, system-name, policy-name  
Name not found.
```

## Probable cause

There was a corruption during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

## SEC-1093

### Message

```
timestamp, [SEC-1093], sequence-number,, ERROR, system-name, New FCS list must have at least one member in common with current FCS list.
```

### Probable cause

The new FCS list does not have a common member with the existing FCS list.

### Recommended action

Resubmit the command with at least one member of the new FCS list in common with the current FCS list.

### Severity

ERROR

## SEC-1094

### Message

```
timestamp, [SEC-1094], sequence-number,, ERROR, system-name, Policy member not found.
```

### Probable cause

There was a corruption during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1095

### Message

```
timestamp, [SEC-1095], sequence-number,, ERROR, system-name, Deleting FCS policy is not allowed.
```

### Probable cause

There was a corruption during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1096

## Message

```
timestamp, [SEC-1096], sequence-number,, ERROR, system-name, Failed to  
delete policy-name. reason-text
```

## Probable cause

There was a corruption during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1097

## Message

```
timestamp, [SEC-1097], sequence-number,, ERROR, system-name, Cannot find  
active-or-defined policy set.
```

## Probable cause

The specified policy could not be found.

## Recommended action

If the message persists, run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

## SEC-1098

### Message

```
timestamp, [SEC-1098], sequence-number,, ERROR, system-name, No  
active-or-defined FCS list.
```

### Probable cause

The specified policy could not be found.

### Recommended action

Run `supportFtp` as needed to set up automatic FTP transfers and then run the `supportSave` command and contact your switch service provider.

### Severity

ERROR

## SEC-1099

### Message

```
timestamp, [SEC-1099], sequence-number,, ERROR, system-name, Please enable  
your switch before running secModeEnable.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

ERROR

## SEC-1100

### Message

```
timestamp, [SEC-1100], sequence-number,, ERROR, system-name, FCS switch  
present. Command terminated.
```

## Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1101

## Message

```
timestamp, [SEC-1101], sequence-number,, ERROR, system-name, Failed to  
enable security on all switches. Please retry later.
```

## Probable cause

The security enable failed on the fabric because one or more switches in the fabric were busy.

## Recommended action

Verify that the security event was planned. If so, run the `secFabricShow` command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

## Severity

ERROR

# SEC-1102

## Message

```
timestamp, [SEC-1102], sequence-number,, ERROR, system-name, Fail to  
download security-data.
```

## Probable cause

The switch failed to download certificate, security database, or policies.

This can happen when the switch does not get enough resources to complete the operation, the fabric has not stabilized, or the policy database is an invalid format.

## Recommended action

Wait for the fabric to become stable and then retry the operation. If the policy database is in an illegal format (with `configDownload`), correct the format and retry the operation.



## Severity

ERROR

# SEC-1104

## Message

```
timestamp, [SEC-1104], sequence-number,, ERROR, system-name, Fail to get  
primary Certificate-or-public-key.
```

## Probable cause

The switch failed to get either the primary certificate or a primary public key.

## Recommended action

1. Verify that the primary switch has a valid certificate installed and retry the operation.
2. If a valid certificate is not installed, install a certificate by following the procedure specified in the *HP StorageWorks Secure Fabric OS user guide*.

## Severity

ERROR

# SEC-1105

## Message

```
timestamp, [SEC-1105], sequence-number,, ERROR, system-name, Fail to  
disable secure mode on all switches.
```

## Probable cause

The switch failed to disable security in the fabric.

This can happen if the switch cannot get the required resources to complete the command and sending to a remote domain fails or the remote domain returns an error.

## Recommended action

Run the `secFabricShow` to verify that all switches in the fabric are in the ready state. Retry the command when all switches are READY.

## Severity

ERROR

## SEC-1106

### Message

```
timestamp, [SEC-1106], sequence-number,, ERROR, system-name, Failed to  
sign message data.
```

### Probable cause

Some PKI objects on the switch are not in a valid state; a signature operation failed.

### Recommended action

1. Run the `pkiShow` command and verify that all PKI objects exist on the switch.
2. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *HP StorageWorks Secure Fabric OS user guide*.

### Severity

ERROR

## SEC-1107

### Message

```
timestamp, [SEC-1107], sequence-number,, INFO, system-name, Stamp is 0.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

### Severity

INFO

## SEC-1108

### Message

```
timestamp, [SEC-1108], sequence-number,, ERROR, system-name, Fail to reset  
stamp on all switches.
```

## Probable cause

A version reset operation failed either because the switch could not get all the required resources to perform the operation or because it failed to send the message to all switches in the fabric.

## Recommended action

1. Verify that the security event was planned. If so, run the `secFabricShow` command to verify that all switches in the fabric are in the ready state.
2. When all switches are in the ready state, retry the operation.

## Severity

ERROR

# SEC-1110

## Message

```
timestamp, [SEC-1110], sequence-number,, ERROR, system-name, FCS list must  
be the first entry in the [Defined Security policies] section. Fail to  
download defined database.
```

## Probable cause

A security policy download was attempted with a defined policy that does not have the FCS policy as the first policy. The FCS policy is required to be the first policy in the defined security database.

## Recommended action

Download a correct configuration with the FCS policy as the first policy in the defined security database.

## Severity

ERROR

# SEC-1111

## Message

```
timestamp, [SEC-1111], sequence-number,, ERROR, system-name, New defined  
FCS list must have at least one member in common with current active FCS  
list. Fail to download defined database.
```

## Probable cause

The defined and active FCS policy list failed to have at least one member in common.

## Recommended action

A new FCS policy list must have at least one member in common with the previous FCS policy.

## Severity

ERROR

## SEC-1112

### Message

```
timestamp, [SEC-1112], sequence-number,, ERROR, system-name, FCS list must be the first entry in the Active Security policies, and the same as the current active FCS list in the switch.
```

### Probable cause

Either a security policy download was attempted with an active policy that does not have the FCS policy as the first policy or the FCS policy is not the same as the current FCS policy on the switch.

### Recommended action

Make sure that the new FCS policy is the same as the current FCS policy on the switch.

### Severity

ERROR

## SEC-1115

### Message

```
timestamp, [SEC-1115], sequence-number,, ERROR, system-name, No primary FCS to failover.
```

### Probable cause

During an attempted `secFcsFailover`, no primary FCS is present in the fabric.

### Recommended action

1. Run the `secFabricShow` command to verify that all switches in fabric are in the ready state.
2. When all switches are in the ready state, retry the operation.

### Severity

ERROR

## SEC-1116

### Message

```
timestamp, [SEC-1116], sequence-number,, ERROR, system-name, Fail to commit failover.
```

### Probable cause

A corruption occurred during the distribution of the security database.

This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1117

## Message

```
timestamp, [SEC-1117], sequence-number,, INFO, system-name, Fail to set  
data.
```

## Probable cause

The switch failed to save the data received by the primary FCS switch. This data can be an FCS password, a non-FCS password, SNMP data, or multiple user authentication data.

## Recommended action

Run the `secFabricShow` command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

## Severity

INFO

# SEC-1118

## Message

```
timestamp, [SEC-1118], sequence-number,, INFO, system-name, Fail to set  
SNMP string.
```

## Probable cause

The SNMP string could not be set.

## Recommended action

Usually this problem is transient. Retry the command.

## Severity

INFO

## SEC-1119

### Message

```
timestamp, [SEC-1119], sequence-number,, INFO, system-name, Secure mode  
has been enabled.
```

### Probable cause

The secure Fabric OS was enabled by the `secModeEnable` command.

### Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-1121

### Message

```
timestamp, [SEC-1121], sequence-number,, ERROR, system-name, Time is out  
of range when text.
```

### Probable cause

The time on the switch is not synchronized with the primary FCS, the data packet is corrupted, or a replay attack is launched on the switch.

### Recommended action

Verify that the security event was planned. If the security event was planned, verify that all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

### Severity

ERROR

## SEC-1122

### Message

```
timestamp, [SEC-1122], sequence-number,, INFO, system-name, Error code:  
domain-ID, error-message.
```

### Probable cause

One of the switches in the fabric could not communicate with the primary FCS.

## Recommended action

Run the `secFabricShow` command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

## Severity

INFO

# SEC-1123

## Message

```
timestamp, [SEC-1123], sequence-number,, INFO, system-name, Security database downloaded by Primary FCS.
```

## Probable cause

The security database was successfully downloaded from the primary FCS.

## Recommended action

No action is required.

## Severity

INFO

# SEC-1124

## Message

```
timestamp, [SEC-1124], sequence-number,, INFO, system-name, Secure Mode is off.
```

## Probable cause

An attempt was made to disable secure mode in a non-secure fabric.

## Recommended action

No action is required.

## Severity

INFO

## SEC-1126

### Message

```
timestamp, [SEC-1126], sequence-number,, INFO, system-name, Secure mode  
has been disabled.
```

### Probable cause

A secure mode disable operation completed successfully.

### Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-1130

### Message

```
timestamp, [SEC-1130], sequence-number,, INFO, system-name, The Primary  
FCS has failed over to a new switch.
```

### Probable cause

An FCS failover operation completed successfully.

### Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-1135

### Message

```
timestamp, [SEC-1135], sequence-number,, INFO, system-name, Secure fabric  
version stamp has been reset.
```

### Probable cause

The version stamp of the secure fabric was reset.



## Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-1136

## Message

```
timestamp, [SEC-1136], sequence-number,, ERROR, system-name, Failed to  
verify signature data-type, MUA, policy, etc.
```

## Probable cause

The receiving switch failed to validate the security database from the primary FCS switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database. This message may also be the result of an internal corruption or a hacker attack to the secure fabric.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch.

## Severity

ERROR

# SEC-1137

## Message

```
timestamp, [SEC-1137], sequence-number,, ERROR, system-name, No signature  
in data-type, MUA, policy, etc.
```

## Probable cause

The receiving switch failed to validate the security database from the primary FCS switch. This message usually indicates that the data package is corrupted, the timestamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database. This message may also be the result of an internal corruption or a hacker attack to the secure fabric.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch.

## Severity

ERROR

# SEC-1138

## Message

```
timestamp, [SEC-1138], sequence-number,, INFO, system-name, Security  
database download received from Primary FCS.
```

## Probable cause

A non-primary FCS switch received a security database download.

## Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-1139

## Message

```
timestamp, [SEC-1139], sequence-number,, ERROR, system-name, The  
RSNMP_POLICY cannot exist without the WSNMP_POLICY.
```

## Probable cause

The receiving switch failed to validate the security database from the primary FCS switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database. This message may also be the result of an internal corruption or a hacker attack to the secure fabric.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch.

## Severity

ERROR

## SEC-1142

### Message

```
timestamp, [SEC-1142], sequence-number,, INFO, system-name, Reject new policies. reason-text.
```

### Probable cause

The new policies are rejected for the reason specified.

### Recommended action

Use proper syntax when entering policy information.

### Severity

INFO

## SEC-1145

### Message

```
timestamp, [SEC-1145], sequence-number,, INFO, system-name, A security admin event has occurred. This message is for information purpose only. The message for individual event is:  
event-specific-data
```

### Probable cause

One of the following occurred:

- The names for the specified policies changed.
- The passwords changed for the specified accounts.
- The SNMP community strings changed.

### Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-1146

### Message

```
timestamp, [SEC-1146], sequence-number,, INFO, system-name, PID changed: state.
```

### Probable cause

The PID format of the switch was changed either to extended-edge PID or from extended-edge PID. If the DCC policies existed, all area ID values either increased or decreased by 16. The values wrap around after 128. If a DCC policy contains an area of 127 before changing to extended-edge PID, then the new area is 15, because of the wraparound.

### Recommended action

No action is required.

### Severity

INFO

## SEC-1153

### Message

```
timestamp, [SEC-1153], sequence-number,, INFO, system-name, Error in RCA: RCS is not supported
```

### Probable cause

Reliable commit service (RCS) is not supported.

### Recommended action

1. Run the `rcsInfoShow` command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.
2. For any switch that does not support RCS, obtain the latest firmware version from your switch supplier, and run the `firmwareDownload` command to upgrade the firmware.
3. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

### Severity

INFO

## SEC-1154

### Message

```
timestamp, [SEC-1154], sequence-number,, INFO, system-name, PID change failed: reason defined-status active-status.
```

## Probable cause

Either the defined or the active policy could not be updated. If the policy database is very large, it might not be able to change the area ID because the new policy database exceeds the maximum size. This message can also occur when the switch is short of memory. The status values can be either `defined`, `active`, or both. A negative value means that a policy set was failed by the daemon.

## Recommended action

Reduce the size of the policy database.

## Severity

INFO

# SEC-1155

## Message

```
timestamp, [SEC-1155], sequence-number,, INFO, system-name, PID change  
failed: reason defined-status active-status.
```

## Probable cause

Either the defined or active policy was too large after modifying the area ID. The status values can be either `defined`, `active`, or both. A negative value means that a policy set was failed by the daemon.

## Recommended action

Reduce the size of the specified policy database.

## Severity

INFO

# SEC-1156

## Message

```
timestamp, [SEC-1156], sequence-number,, INFO, system-name, Change failed:  
reason defined-status active-status.
```

## Probable cause

The security daemon is busy. The status values can be either `defined`, `active`, or both. A negative value means that a policy set was failed by the daemon.

## Recommended action

For the first reject, wait a few minutes and then resubmit the transaction. Fabric-wide commands may take a few minutes to propagate throughout the fabric. Wait a few minutes between executing commands so that your commands do not overlap in the fabric.

## Severity

INFO

## SEC-1157

### Message

```
timestamp, [SEC-1157], sequence-number,, INFO, system-name, PID Change  
failed: reason defined-status active-status.
```

### Probable cause

The provisioning resources for a security policy failed due to low memory or internal error. The status values can be either *defined*, *active*, or both. A negative value means that a policy set was failed by the daemon.

### Recommended action

1. Retry the failed command.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

INFO

## SEC-1158

### Message

```
timestamp, [SEC-1158], sequence-number,, INFO, system-name, Invalid name  
policy-or-switch-name.
```

### Probable cause

The specified name is invalid. The *name* can be a policy name or a switch name.

### Recommended action

Enter a valid name.

### Severity

INFO

## SEC-1159

### Message

```
timestamp, [SEC-1159], sequence-number,, INFO, system-name, Non_Reachable  
domain domain-ID.
```

## Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

INFO

# SEC-1160

## Message

```
timestamp, [SEC-1160], sequence-number,, INFO, system-name, Duplicate port  
port-ID in port list (port-list).
```

## Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch.

## Severity

INFO

# SEC-1163

## Message

```
timestamp, [SEC-1163], sequence-number,, ERROR, system-name, System is  
already in secure mode. Lockdown option cannot be applied.
```

## Probable cause

The lockdown option was attempted while the fabric was already in secure mode.

## Recommended action

Do not use the lockdown option with `secModeEnable` when switch is already in secure mode.

## Severity

ERROR

# SEC-1164

## Message

```
timestamp, [SEC-1164], sequence-number,, ERROR, system-name, Lockdown  
option cannot be applied on a non-FCS switch.
```

## Probable cause

The attempt to enable security was made on a switch not present in the FCS list.

## Recommended action

Add the switch into the FCS policy list when using the lockdown option to enable security.

## Severity

ERROR

# SEC-1165

## Message

```
timestamp, [SEC-1165], sequence-number,, ERROR, system-name, Low memory,  
failed to enable security on all switches.
```

## Probable cause

The system is low on memory.

## Recommended action

Wait a few minutes and try the command again.

## Severity

ERROR

# SEC-1166

## Message

```
timestamp, [SEC-1166], sequence-number,, ERROR, system-name, Non FCS tries  
to commit failover.
```

## Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.



## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1167

## Message

```
timestamp, [SEC-1167], sequence-number,, ERROR, system-name, Another FCS failover is in process. Command terminated.
```

## Probable cause

This failover attempt cannot proceed because another failover is already in progress.

## Recommended action

1. Verify that the security event was planned.
2. If the security event was planned, retry the FCS failover after the current failover has completed, if this switch should become primary FCS.
3. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

ERROR

# SEC-1168

## Message

```
timestamp, [SEC-1168], sequence-number,, ERROR, system-name, Primary FCS failover is busy. Please retry later.
```

## Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

## Severity

ERROR

# SEC-1170

## Message

```
timestamp, [SEC-1170], sequence-number,, INFO, system-name, This command must be executed on the Primary FCS switch, the first reachable switch in the FCS list.
```

## Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

INFO

# SEC-1171

## Message

```
timestamp, [SEC-1171], sequence-number,, ERROR, system-name, Disabled secure mode due to invalid security object.
```

## Probable cause

The switch is segmented, and secure mode is disabled on the switch because no license or no PKI objects are present.

## Recommended action

1. Run the `pkiShow` command to check whether all PKI objects exist. If they do not exist, run the `pkiCreate` command to create them for the switch.
2. Run the `licenseAdd` command to install the required license key. Refer to your switch supplier to obtain a license if you do not have one.

## Severity

ERROR

## SEC-1172

### Message

```
timestamp, [SEC-1172], sequence-number,, ERROR, system-name, Failed to identify role.
```

### Probable cause

The switch is unable to determine its role (primary FCS or backup FCS) in the secure fabric.

### Recommended action

1. Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric.
2. When verification is complete, retry the operation.

### Severity

ERROR

## SEC-1173

### Message

```
timestamp, [SEC-1173], sequence-number,, ERROR, system-name, Lost contact with Primary FCS switch.
```

### Probable cause

The switch lost contact with the primary FCS switch in the secure fabric. This could be caused by the primary FCS being disabled.

### Recommended action

If the primary FCS was disabled intentionally, no action is required; if not, check the primary FCS.

### Severity

ERROR

## SEC-1174

### Message

```
timestamp, [SEC-1174], sequence-number,, ERROR, system-name, Failed to set FCS-or-non-FCS password.
```

### Probable cause

The FCS or non-FCS password could not be set.

## Recommended action

1. Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric.
2. When verification is complete, retry the operation.

## Severity

ERROR

# SEC-1175

## Message

```
timestamp, [SEC-1175], sequence-number,, ERROR, system-name, Failed to  
install zone data.
```

## Probable cause

The zone database could not be installed on the switch.

## Recommended action

1. Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric.
2. When verification is complete, retry the operation.

## Severity

ERROR

# SEC-1176

## Message

```
timestamp, [SEC-1176], sequence-number,, ERROR, system-name, Failed to  
generate new version stamp.
```

## Probable cause

The primary FCS failed to generate a new version stamp because the fabric is not stable.

## Recommended action

1. Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric.
2. When verification is complete, retry the operation.

## Severity

ERROR

## SEC-1180

### Message

```
timestamp, [SEC-1180], sequence-number,, INFO, system-name, Added account  
user-name with role-name authorization.
```

### Probable cause

The specified new account was created.

### Recommended action

No action is required.

### Severity

INFO

## SEC-1181

### Message

```
timestamp, [SEC-1181], sequence-number,, INFO, system-name, Deleted  
account user-name
```

### Probable cause

The specified account was deleted.

### Recommended action

No action is required.

### Severity

INFO

## SEC-1182

### Message

```
timestamp, [SEC-1182], sequence-number,, INFO, system-name, Recovered  
number-of accounts.
```

### Probable cause

The specified number of accounts were recovered from backup.

### Recommended action

No action is required.

## Severity

INFO

# SEC-1183

## Message

```
timestamp, [SEC-1183], sequence-number,, ERROR, system-name, Policy to  
binary conversion error: Port port-number is out range.
```

## Probable cause

A security database conversion failed because of an invalid value.

## Recommended action

1. Retry the command with a valid value.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# SEC-1184

## Message

```
timestamp, [SEC-1184], sequence-number,, INFO, system-name, Radius config  
change, action action, server ID server.
```

## Probable cause

The specified action was applied to the specified RADIUS server configuration. The possible actions are ADD, REMOVE, CHANGE, and MOVE.

## Recommended action

No action is required.

## Severity

INFO

# SEC-1185

## Message

```
timestamp, [SEC-1185], sequence-number,, INFO, system-name, action switch  
DB.
```

## Probable cause

The switch database was enabled or disabled as the secondary AAA when RADUIS is the primary AAA mechanism.

## Recommended action

No action is required.

## Severity

INFO

# SEC-1186

## Message

```
timestamp, [SEC-1186], sequence-number,, INFO, system-name, action Radius Configuration.
```

## Probable cause

The RADIUS configuration was enabled or disabled as the primary AAA mechanism.

## Recommended action

No action is required.

## Severity

INFO

# SEC-1187

## Message

```
timestamp, [SEC-1187], sequence-number,, INFO, system-name, Security violation: Unauthorized switch switch-wwn tries to join secure fabric.
```

## Probable cause

An SCC security violation was reported. The specified unauthorized switch attempted to join the secure fabric.

## Recommended action

1. Check the switch connection control policy (the SCC policy specifies the WWNs of switches allowed in the fabric) to verify which switches are allowed in the fabric.
2. If the switch is allowed in the fabric but is not included in the SCC policy, add the switch to the policy.
3. If the switch is not allowed access to the fabric, the message is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

## Severity

INFO

# SEC-1188

## Message

```
timestamp, [SEC-1188], sequence-number,, INFO, system-name, Security violation: Unauthorized device device-node-name tries to flogin to area port-number of switch switch-wwn.
```

## Probable cause

A DCC security violation was reported. The specified device attempted to log in using fabric login (FLOGI) to an unauthorized port. The DCC policy correlates specific devices to specific port locations. If the device changes connected port, it is not allowed to log in.

## Recommended action

1. Check the DCC policy and verify that the specified device is allowed in the fabric and is included in the DCC policy.
2. If the specified device not included in the policy, add it to the policy.
3. If the host is not allowed access to the fabric, the message is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

## Severity

INFO

# SEC-1189

## Message

```
timestamp, [SEC-1189], sequence-number,, INFO, system-name, Security violation: Unauthorized host with IP address IP-address tries to do SNMP write operation.
```

## Probable cause

An SNMP security violation was reported. The specified unauthorized host attempted to perform a write SNMP operation.

## Recommended action

1. Check the WSNMP policy and verify which hosts are allowed access to the fabric through SNMP.
2. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy.
3. If the host is not allowed access to the fabric, the message is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

## Severity



INFO

## SEC-1190

### Message

```
timestamp, [SEC-1190], sequence-number,, INFO, system-name, Security  
violation: Unauthorized host with IP address IP-address tries to do SNMP  
read operation.
```

### Probable cause

An SNMP security violation was reported. The specified unauthorized host attempted to perform a read SNMP operation.

### Recommended action

1. Check the RSNMP policy to verify that hosts allowed access to the fabric through SNMP read operations are included in the RSNMP policy.
2. If the host is allowed access but is not included in the RSNMP policy, add the host to the policy.
3. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

### Severity

INFO

## SEC-1191

### Message

```
timestamp, [SEC-1191], sequence-number,, INFO, system-name, Security  
violation: Unauthorized host with IP address IP-address tries to establish  
HTTP connection.
```

### Probable cause

An HTTP security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

### Recommended action

1. Check whether the host IP address specified in the message can be used to manage the fabric through an HTTP connection.
2. If the host can be used to manage the fabric, add the host IP address to the HTTP policy of the fabric.
3. If the host is not allowed access to the fabric, the message is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

### Severity

INFO

## SEC-1192

### Message

```
timestamp, [SEC-1192], sequence-number,, INFO, system-name, Security  
violation: Login failure attempt via connection-method.
```

### Probable cause

A serial or modem login security violation was reported. The wrong password was used while trying to log in through a serial or modem connection; the login failed.

### Recommended action

Use the correct password.

### Severity

INFO

## SEC-1193

### Message

```
timestamp, [SEC-1193], sequence-number,, INFO, system-name, Security  
violation: Login failure attempt via connection-method. IP Addr:  
IP-address
```

### Probable cause

The specified login security violation was reported. The wrong password was used while trying to log in through the specified connection method; the login failed.

### Recommended action

The error message lists the violating IP address. Verify that this IP address is being used by a valid switch admin. Use the correct password.

### Severity

INFO

## SEC-1194

### Message

```
timestamp, [SEC-1194], sequence-number,, WARNING, system-name, This switch  
does not have all the required PKI objects correctly installed.
```

## Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

WARNING

# SEC-1195

## Message

```
timestamp, [SEC-1195], sequence-number, , WARNING, system-name, This switch  
has no component license.
```

## Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

## Severity

WARNING

# SEC-1196

## Message

```
timestamp, [SEC-1196], sequence-number, , WARNING, system-name, Switch does  
not have all default account names.
```

## Probable cause

The default switch accounts `admin` and `user` did not exist on the switch when attempting to enable security.

## Recommended action

Reset the default `admin` and `user` account names on the switch that reported the warning and retry enabling security.

## Severity

WARNING

# SEC-1197

## Message

```
timestamp, [SEC-1197], sequence-number,, INFO, system-name, Changed  
account user-name.
```

## Probable cause

The specified account changed.

## Recommended action

No action is required.

## Severity

INFO

# SEC-1198

## Message

```
timestamp, [SEC-1198], sequence-number,, INFO, system-name, Security  
violation: Unauthorized host with IP address IP-address tries to establish  
API connection.
```

## Probable cause

An API security violation was reported. The specified unauthorized host attempted to establish an API connection.

## Recommended action

1. Check to see whether the host IP address specified in the message can be used to manage the fabric through an API connection.
2. If the host IP address can be used to manage the fabric, add the host IP address to the API policy of the fabric.
3. If the host is not allowed access to the fabric, the message is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

## Severity

INFO

## SEC-1199

### Message

```
timestamp, [SEC-1199], sequence-number,, INFO, system-name, Security violation: Unauthorized access to serial port of switch switch-instance.
```

### Probable cause

A serial connection policy security violation was reported. An attempt was made to access the serial console on the specified switch instance when it was disabled.

### Recommended action

1. Check to see whether an authorized access attempt is being made on the console.
2. If an authorized access attempt is being made, add the switch WWN to the serial policy.
3. If the host is not allowed access to the fabric, the message is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

### Severity

INFO

## SEC-1200

### Message

```
timestamp, [SEC-1200], sequence-number,, INFO, system-name, Security violation: MS command is forwarded from non-primary FCS switch.
```

### Probable cause

An MS forward security violation was reported. A management server command was forwarded from a non-primary FCS switch.

### Recommended action

1. Check the MS policy and verify that the connection is allowed.
2. If the connection is allowed but not specified, enable the connection in the MS policy.
3. If the MS policy does not allow the connection, the message is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

### Severity

INFO

# SEC-1201

## Message

```
timestamp, [SEC-1201], sequence-number,, INFO, system-name, Security  
violation: MS device device-wwn operates on non-primary FCS switch.
```

## Probable cause

An MS operation security violation was reported. An MS device operation occurred on a non-primary FCS switch.

## Recommended action

1. Check the management server policy and verify that the connection is allowed.
2. If the connection is allowed but not specified, enable the connection is MS policy.
3. If the MS policy does not allow the connection, the message is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

## Severity

INFO

# SEC-1202

## Message

```
timestamp, [SEC-1202], sequence-number,, INFO, system-name, Security  
violation: Unauthorized access from MS device node name device-node-name,  
device port name device-port-name.
```

## Probable cause

An MS security violation was reported. The unauthorized device specified in the message attempted to establish a connection.

## Recommended action

1. Check the MS server policy and verify that the connection is allowed.
2. If the connection is allowed but not specified, enable the connection in the MS policy.
3. If the MS policy does not allow the connection, the message is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

## Severity

INFO

## SEC-1250

### Message

```
timestamp, [SEC-1250], sequence-number,, WARNING, system-name, DCC  
enforcement API failed: failed-action err=status, key=data
```

### Probable cause

An internal error caused the DCC policy enforcement to fail.

### Recommended action

1. Retry the failed security command.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

WARNING

## SEC-1251

### Message

```
timestamp, [SEC-1251], sequence-number,, ERROR, system-name, Policy to  
binary conversion error: text-message value.
```

### Probable cause

The security database conversion failed because of invalid values. The reason is specified in the `text-message` variable and the faulty value is printed in the `value` variable.

### Recommended action

1. Retry the failed security command.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

ERROR

## SEC-1253

### Message

```
timestamp, [SEC-1253], sequence-number,, ERROR, system-name, Bad DCC  
interface state during phase, state=state.
```

## Probable cause

An internal error caused the DCC policy update to fail in the provision, commit, or cancel phases.

## Recommended action

1. Retry the failed security command.
2. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# SEC-1300

## Message

```
timestamp, [SEC-1300], sequence-number, , INFO, system-name, This switch is  
in VcEncode mode. Security is not supported.
```

## Probable cause

The switch is set up with VC-encoded mode.

## Recommended action

Turn off VC-encoded mode before enabling security.

## Severity

INFO

# SEC-1301

## Message

```
timestamp, [SEC-1301], sequence-number, , INFO, system-name, This switch is  
in interop mode. Security is not supported.
```

## Probable cause

The switch is interop mode enabled.

## Recommended action

Disable interop-mode using the `interopMode` command before enabling the Secure Fabric OS feature.

## Severity

INFO



## SEC-1302

### Message

```
timestamp, [SEC-1302], sequence-number,, INFO, system-name, This switch  
does not have all the required PKI objects correctly installed.
```

### Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

### Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

### Severity

INFO

## SEC-1303

### Message

```
timestamp, [SEC-1303], sequence-number,, INFO, system-name, This software  
version does not support security.
```

### Probable cause

The currently installed software version does not support the HP StorageWorks Secure Fabric OS feature.

### Recommended action

Run the `firmwareDownload` command to update the firmware to the latest version for your specific switch. Verify that the firmware you are installing supports the HP StorageWorks Secure Fabric OS feature.

### Severity

INFO

## SEC-1304

### Message

```
timestamp, [SEC-1304], sequence-number,, INFO, system-name, This switch  
has no security license.
```

## Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

## Severity

INFO

# SEC-1305

## Message

```
timestamp, [SEC-1305], sequence-number,, INFO, system-name, This switch  
has no zoning license.
```

## Probable cause

A corruption occurred during the distribution of the security database. This can occur only when the primary FCS is distributing the security database to the other switches in the fabric and local validation finds that an error occurred in the security database. This is a rare occurrence.

## Recommended action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

## Severity

INFO

# SEC-1306

## Message

```
timestamp, [SEC-1306], sequence-number,, INFO, system-name, Failed to  
verify certificate with root CA.
```

## Probable cause

The certificate could not be verified with root certificate authority (CA). This can happen if an unauthorized switch that is not certified by a trusted root certificate authority (CA) or a root CA certificate does not exist on the switch, tries to access the fabric.

## Recommended action

1. Run the `pkiShow` command and verify that all PKI objects exist on the switch.

2. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *HP StorageWorks Fabric OS user guide*.
3. If PKI objects are valid, verify that an unauthorized switch is not trying to access the fabric.

## Severity

INFO

# SEC-1307

## Message

```
timestamp, [SEC-1307], sequence-number,, INFO, system-name, Got response  
from Radius server radius-server-identity.
```

## Probable cause

After some servers timed out, the specified RADIUS server responded to a switch request.

## Recommended action

If the message appears frequently, move the specified server to the top of the server configuration list.

## Severity

INFO

# SEC-1308

## Message

```
timestamp, [SEC-1308], sequence-number,, INFO, system-name, All Radius  
servers have failed to respond.
```

## Probable cause

All servers in the RADIUS configuration failed to respond to a switch request within the specified timeout.

## Recommended action

Verify that the switch has proper network connectivity to the specified RADIUS servers, and the servers are correctly configured.

## Severity

INFO

# SEC-3001

## Message

```
timestamp, [SEC-3001], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
security mode state-change:-enabled-or-disabled.
```

## Probable cause

The security mode of the fabric was either enabled or disabled.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-3002

## Message

```
timestamp, [SEC-3002], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
NONE
```

## Probable cause

The specified security event occurred. The event can be:

- An FCS failover.
- A security policy being activated
- A security policy being saved
- A security policy being aborted
- A non-FCS password being changed
- A temporary password being set or reset

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

## SEC-3003

### Message

```
timestamp, [SEC-3003], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
Create policy-name policy, with member-list entries.
```

### Probable cause

A new security policy with entries was created. When you use a wildcard (for example, an asterisk) in creating a policy, the audit report displays the wildcard in the Event Info field.

### Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-3004

### Message

```
timestamp, [SEC-3004], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
Create policy-name policy.
```

### Probable cause

A new security policy was created. When you use a wildcard (for example, an asterisk) in creating member for a policy, the audit report displays the wildcard in the Event Info field.

### Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

# SEC-3005

## Message

```
timestamp, [SEC-3005], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
Add members [members-added] to policy policy-name.
```

## Probable cause

New members were added to a security policy. When you use a wildcard (for example, an asterisk) in adding members to a policy, the audit report displays the wildcard in the Event Info field.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-3006

## Message

```
timestamp, [SEC-3006], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
Remove members [members-removed] from policy policy-name.
```

## Probable cause

A user removed the specified members from the security policy. When a wildcard is used (for example, an asterisk) in removing members from a policy, the audit report displays the wildcard in the Event Info field.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

## SEC-3007

### Message

```
timestamp, [SEC-3007], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
Delete policy deleted-policy-name.
```

### Probable cause

The user deleted the specified security policy.

### Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-3008

### Message

```
timestamp, [SEC-3008], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
FCS moved from position [old-FCS-position] to [new-FCS-position].
```

### Probable cause

The FCS list was modified. One of the members of the list was moved to a new position in the list.

### Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

### Severity

INFO

## SEC-3009

### Message

```
timestamp, [SEC-3009], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
Security Transaction aborted.
```

## Probable cause

The pending security transaction was aborted.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-3010

## Message

```
timestamp, [SEC-3010], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
Reset [event-specific-information] security stat(s).
```

## Probable cause

The specified user reset all the security statistics.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-3011

## Message

```
timestamp, [SEC-3011], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
Reset stat-name stat on domains domain-IDs.
```

## Probable cause

The specified user has reset a security statistic on the specified domains.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.



## Severity

INFO

# SEC-3012

## Message

```
timestamp, [SEC-3012], sequence-number, AUDIT, INFO, system-name, User:
user-name, role: user-role, Event: event-name, status: event-status, Info:
Passwd set/reset on domain [domain-ID] for account(s) account-name.
```

## Probable cause

The specified user reset the password for the specified user accounts.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-3013

## Message

```
timestamp, [SEC-3013], sequence-number, AUDIT, INFO, system-name, User:
user-name, role: user-role, Event: event-name, status: event-status, Info:
Version is reset.
```

## Probable cause

The specified user reset the security version stamp.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-3014

## Message

```
timestamp, [SEC-3014], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
event-option server event-data.
```

## Probable cause

The specified user changed the RADIUS configuration.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-3015

## Message

```
timestamp, [SEC-3015], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
event-option server server-name to position new-position.
```

## Probable cause

The specified user changed the RADIUS configuration.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-3016

## Message

```
timestamp, [SEC-3016], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
event-option server server-ID attributes.  
New values: changed-values
```

## Probable cause

The specified user changed the RADIUS configuration.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

# SEC-3017

## Message

```
timestamp, [SEC-3017], sequence-number, AUDIT, INFO, system-name, User:  
user-name, role: user-role, Event: event-name, status: event-status, Info:  
Radius server-state
```

## Probable cause

The specified user changed the RADIUS configuration.

## Recommended action

1. Verify that the security event was planned. If the security event was planned, no action is required.
2. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

## Severity

INFO

---

# Simple network management protocol error messages

# SNMP-1001

## Message

```
timestamp, [SNMP-1001], sequence-number,, ERROR, system-name, SNMP service  
is not available reason.
```

## Probable cause

Indicates that the SNMP service could not be started because of the specified *reason*. You cannot query the switch through SNMP.

## Recommended action

Verify that the IP address for the Ethernet and Fibre Channel interface is set correctly. If the specified *reason* is an initialization failure, the switch requires a reboot.

## Severity

ERROR

# SNMP-1002

## Message

```
timestamp, [SNMP-1002], sequence-number,, ERROR, system-name, SNMP  
error-details initialization failed.
```

## Probable cause

The initialization of the SNMP service failed; you cannot query the switch through SNMP.

## Recommended action

Reboot or power cycle the switch. This initializes SNMP.

## Severity

ERROR

# SNMP-1003

## Message

```
timestamp, [SNMP-1003], sequence-number,, ERROR, system-name, Distribution  
of Community Strings to Secure Fabric failed.
```

## Probable cause

The changes in the SNMP community strings could not be propagated to other switches in the secure fabric.

## Recommended action

Retry changing the SNMP community strings from the primary switch.

## Severity

ERROR

# SNMP-1004

## Message

```
timestamp, [SNMP-1004], sequence-number,, ERROR, system-name, Incorrect  
SNMP configuration.
```

## Probable cause

The SNMP configuration is incorrect and the SNMP service does not work correctly.

## Recommended action

Try changing the SNMP configuration back to the default.

## Severity

ERROR

---

# SupportSave command error messages

## SS-1000

## Message

```
timestamp, [SS-1000], sequence-number,, INFO, system-name, supportSave has  
ftp'ed support information to the host with IP address host-IP.
```

## Probable cause

The supportSave command was used to transfer support information to a remote FTP location.

## Recommended action

No action is required.

## Severity

INFO

## SS-1001

## Message

```
timestamp, [SS-1001], sequence-number,, WARNING, system-name,  
supportSave's ftp operation to host IP address host-IP aborted.
```

## Probable cause

An FTP error occurred during execution of the supportSave command.

## Recommended action

1. Check the FTP server and settings.
2. Run the `supportFtp` command to set the FTP parameters.
3. After the FTP problem is corrected, rerun the `supportSave` command.

## Severity

WARNING

---

# Software upgrade library error messages

## SULB-1001

### Message

```
timestamp, [SULB-1001], sequence-number,, WARNING, system-name,  
Firmwaredownload command has started.
```

### Probable cause

The `firmwareDownload` command started. This process can take some time; wait until the process is complete before initiating any new commands to the system.

## Recommended action

1. Do not fail over or power down the system during firmware upgrade. Allow the `firmwareDownload` command to continue without disruption.
2. Run the `firmwareDownloadStatus` command for more information.

## Severity

WARNING

## SULB-1002

### Message

```
timestamp, [SULB-1002], sequence-number,, INFO, system-name,  
Firmwaredownload command has completed successfully.
```

### Probable cause

The `firmwareDownload` command completed successfully and loaded firmware to both the control processors (CPs).

## Recommended action

No action is required. The `firmwareDownload` command has completed as expected. Run the `firmwareDownloadStatus` command for more information.

## Severity

INFO

# SULB-1003

## Message

```
timestamp, [SULB-1003], sequence-number,, INFO, system-name,  
Firmwarecommit has started.
```

## Probable cause

The `FirmwareCommit` command started to update the secondary partition.

## Recommended action

No action is required. Run the `firmwareDownloadStatus` command for more information.

## Severity

INFO

# SULB-1005

## Message

```
timestamp, [SULB-1005], sequence-number,, INFO, system-name, Current  
Active CP is preparing to failover.
```

## Probable cause

The forced failover was successful and the standby CP is now the active CP.

## Recommended action

No action is required. The `firmwareDownload` command is progressing as expected. Run the `firmwareDownloadStatus` command for more information.

## Severity

INFO

# SULB-1006

## Message

```
timestamp, [SULB-1006], sequence-number,, INFO, system-name, Forced  
failover succeeded. New Active CP is running new firmware.
```

## Probable cause

The previous standby became the active CP and is running the new firmware version.

## Recommended action

No action is required. The `firmwareDownload` command is progressing as expected. Run the `firmwareDownloadStatus` command for more information.

## Severity

INFO

# SULB-1007

## Message

```
timestamp, [SULB-1007], sequence-number,, INFO, system-name, Standby CP  
reboots.
```

## Probable cause

The standby CP reboots.

## Recommended action

No action is required. The `firmwareDownload` command is progressing as expected. Run the `firmwareDownloadStatus` command for more information.

## Severity

INFO

# SULB-1008

## Message

```
timestamp, [SULB-1008], sequence-number,, INFO, system-name, Standby CP  
booted successfully with new firmware.
```

## Probable cause

The standby CP has rebooted successfully.

## Recommended action

No action is required. The `firmwareDownload` command is progressing as expected. Run the `firmwareDownloadStatus` command for more information.

## Severity

INFO



# SULB-1009

## Message

```
timestamp, [SULB-1009], sequence-number,, INFO, system-name,  
FirmwareDownload command failed (0xfirmwareDownload-error-code).
```

## Probable cause

The firmware download failed. The additional error code provides debugging information.

The `firmwareDownload` error code contains two bytes. The first byte contains the upgrade error message code, as indicated in [Table 6](#); the second byte may contain either the reason code (the failure cause) or the state code (where the failure occurs), also as indicated in [Table 6](#). Retrieve the error code by running the `firmwareDownloadStatus` command or through the `errShow` and `errDump` commands.

For example, the following entry indicates that the `firmwareDownload` failed in `SUS_SBY_FS_CHECK` (0x2e) state because the Standby CP failed to reboot (0x66):

```
Switch: 0, Info SULIB-FWDL_FAIL, 4, FirmwareDownload command failed  
(status=0x662e).
```

The following entry indicates that the `firmwareDownload` failed (0x44) because firmware has not been committed (0x1e):

```
Switch: 0, Info SULIB-FWDL_FAIL, 4, FirmwareDownload command failed  
(status=0x441e)
```

[Table 6](#) lists the upgrade messages and their associated codes.

**Table 6** Upgrade messages and code values

Upgrade message	Code
Image is up-to-date. No need to download.	0xF
Boot environment variable is inconsistent.	0x10
Bootenv OSRootPartition is inconsistent.	0x11
Can't access package list (.plist) file.	0x12
RPM database is inconsistent.	0x13
Ran out of memory.	0x14
FirmwareDownload failed due to out of disk space or timeout.	0x15
Failed to create firmware version file.	0x16
Unexpected system error.	0x17
Error in getting lock device.	0x18
Error in releasing lock device.	0x19
Firmwarecommit failed.	0x1a

**Table 6** Upgrade messages and code values (continued)

Upgrade message	Code
Firmware directory structure is not compatible.	0x1b
Failed to load kernel image.	0x1c
Bootenv OSLoader is inconsistent.	0x1d
Firmwaredownload failed because new image has not been committed.	0x1e
Firmwarerestore failed.	0x1f
Both images are mounted to the same device.	0x20
Error in removing packages.	0x21
Firmwaredownload is already in progress.	0x22
Firmwaredownload timeout.	0x23
Firmwaredownload sanity check failed.	0x30
Sanity check failed because system is non-redundant.	0x31
Sanity check failed because firmwareDownload is already in progress.	0x32
Sanity check failed because FABRIC OS is disabled on Active CP.	0x33
Sanity check failed because HAMD is disabled on Active CP.	0x34
Sanity check failed because firmwareDownload is already in progress.	0x35
Sanity check failed because FABRIC OS is disabled on Standby CP.	0x36
Sanity check failed because HAMD is disabled on Standby CP.	0x37
Firmwaredownload failed on Standby CP.	0x40
Firmwaredownload failed on Standby CP.	0x41
Firmwaredownload failed on Standby CP.	0x42
Firmwarecommit failed on Standby CP.	0x43
Firmwaredownload failed.	0x44

**Table 6** Upgrade messages and code values (continued)

Upgrade message	Code
Firmwaredownload failed due to Standby CP timeout.	0x50
Unable to check firmware version due to Standby CP timeout.	0x51
Firmwaredownload failed due to Standby CP timeout.	0x52
Firmwaredownload failed due to Standby CP timeout.	0x53
Standby CP failed to reboot and was not responding.	0x54
Firmwarecommit failed due to Standby CP timeout.	0x55
Unable to check firmware version due to Standby CP timeout.	0x56
Unable to restore the original firmware due to Standby CP timeout.	0x57
Standby CP failed to reboot and was not responding.	0x58
Unable to check firmware version due to Standby CP timeout.	0x59
Sanity check failed because firmwareDownload is already in progress.	0x60
Sanity check failed because firmwareDownload is already in progress.	0x61
NOT USED	0x62
System Error.	0x63
Active CP forced failover succeeded. Now this CP becomes Active.	0x64
Standby CP booted up.	0x65
Standby CP failed to reboot.	0x66
Standby rebooted successfully.	0x67
Standby failed to reboot.	0x68
Firmwarecommit has started to restore the secondary partition.	0x69

**Table 6** Upgrade messages and code values (continued)

Upgrade message	Code
Local CP is restoring its secondary partition.	0x6a
Unable to restore the secondary partition. Please use <code>firmwaredownloadstats</code> and <code>firmwareshow</code> to see firmware status.	0x6b
Firmwaredownload has started on Standby CP. It may take up to 10 minutes.	0x6c
Firmwaredownload has completed successfully on Standby CP.	0x6d
Standby CP reboots.	0x6e
Standby CP failed to boot up.	0x6f
Standby CP booted up with new firmware.	0x70
Standby CP failed to boot up with new firmware.	0x71
Firmwaredownload has completed successfully on Standby CP.	0x72
Firmwaredownload has started on Standby CP. It may take up to 10 minutes.	0x73
Firmwaredownload has completed successfully on Standby CP.	0x74
Standby CP reboots.	0x75
Standby CP failed to reboot.	0x76
Firmwarecommit has started on Standby CP.	0x77
Firmwarecommit has completed successfully on Standby CP.	0x78
Standby CP booted up with new firmware.	0x79
Standby CP failed to boot up with new firmware.	0x7a
Firmwarecommit has started on both Active and Standby CPs.	0x7b
Firmwarecommit has completed successfully on Active CP.	0x7c
Firmwarecommit failed on Active CP.	0x7d

**Table 6** Upgrade messages and code values (continued)

Upgrade message	Code
The original firmware has been restored successfully on Standby CP.	0x7e
Unable to restore the original firmware on Standby CP.	0x7f
Standby CP reboots.	0x80
Standby CP failed to reboot.	0x81
Standby CP booted up with new firmware.	0x82
Standby CP failed to boot up with new firmware.	0x83
An unexpected reboot occurred during firmwareDownload. The command is aborted.	0x84
Standby CP was not responding. The command is aborted.	0x85
Firmwarecommit has started on both CPs. Please use firmwaredownloadstatus and firmwareshow to see the firmware status.	0x86
Firmwarecommit has started on the local CP. Please use firmwaredownloadstatus and firmwareshow to see the firmware status.	0x87
Firmwarecommit has started on the remote CP. Please use firmwaredownloadstatus and firmwareshow to see the firmware status.	0x88
Please use firmwaredownloadstatus and firmwareshow to see the firmware status.	0x89
Firmwaredownload command has completed successfully.	0x8a
The original firmware has been restored successfully.	0x8b
Remote CP is restoring its secondary partition.	0x8c
Local CP is restoring its secondary partition.	0x8d
Remote CP is restoring its secondary partition.	0x8e
Firmwaredownload has started.	0x8f
Firmwarecommit has started.	0x90

**Table 6** Upgrade messages and code values (continued)

Upgrade message	Code
Firmwaredownload has completed successfully.	0x91
Firmwarecommit has completed successfully.	0x92
Firmwarecommit has started to restore the secondary partition.	0x93
Firmwarecommit failed.	0x94
The secondary partition has been restored successfully.	0x95

Table 7 lists upgrade states and their associated codes.

**Table 7** Upgrade state and code values

Upgrade state	Code
SUS_PEER_CHECK_SANITY	0x21
SUS_PEER_FWDL_BEGIN	0x22
SUS_SBY_FWDL_BEGIN	0x23
SUS_PEER_REBOOT	0x24
SUS_SBY_REBOOT	0x25
SUS_SBY_FABOS_OK	0x26
SUS_PEER_FS_CHECK	0x27
SUS_SELF_FAILOVER	0x28
SUS_SBY_FWDL1_BEGIN	0x29
SUS_SELF_FWDL_BEGIN	0x2a
SUS_SELF_COMMIT	0x2b
SUS_SBY_FWC_BEGIN	0x2c
SUS_SBY_COMMIT	0x2d
SUS_SBY_FS_CHECK	0x2e
SUS_ACT_FWC_BEGIN	0x2f
SUS_PEER_RESTORE_BEGIN	0x30
SUS_SBY_RESTORE_BEGIN	0x31

**Table 7** Upgrade state and code values (continued)

Upgrade state	Code
SUS_PEER_FWC_BEGIN	0x32
SUS_PEER_FS_CHECK1	0x33
SUS_FINISH	0x34
SUS_COMMIT	0x35

## Recommended action

Run the `firmwareDownload status` command for more information. Refer to the *HP StorageWorks Fabric OS 4.x procedures user guide* for troubleshooting information.

## Severity

INFO

# SULB-1010

## Message

```
timestamp, [SULB-1010], sequence-number,, INFO, system-name,  
Firmwarecommit failed (status=0xfirmwarecommit-error-code).
```

## Probable cause

A firmware commit failed to update the secondary partition.

## Recommended action

Run the `firmwareCommit` command with the `-d` option.

## Severity

INFO

---

# Switch driver module error messages

# SWCH-1001

## Message

```
timestamp, [SWCH-1001], sequence-number,, ERROR, system-name, Switch is  
not in ready state - Switch enable failed switch status= 0xswitch-status,  
c_flags = 0xswitch-control-flags
```

## Probable cause

The switch was enabled before it was ready.

## Recommended action

1. If the message persists, run `supportFtp` as needed to set up automatic FTP transfers.
2. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# SWCH-1002

## Message

```
timestamp, [SWCH-1002], sequence-number,, INFO, system-name, Security violation: Unauthorized device wwn-name-of-device tries to flogin to port port-number
```

## Probable cause

The device is not present in the authorized profile list.

## Recommended action

1. Verify that the device is authorized to log in to the switch. If the device is authorized, run the `secPolicyDump` command to verify whether the specified device WWN is listed.
2. If it is not listed, run the `secPolicyAdd` command to add this device to an existing policy.

## Severity

INFO

# SWCH-1003

## Message

```
timestamp, [SWCH-1003], sequence-number,, ERROR, system-name, Slot ENABLED but Not Ready during recovery, disabling slot = slot-number(return-value)
```

## Probable cause

The slot state was detected as inconsistent during failover or recovery.

## Recommended action

On a Core Switch 2/64 or SAN Director 2/128 switch, first run the `slotPowerOff` command and then run the `slotPowerOn` command.

On a SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, or SAN Switch 4/32 switch, reboot or power cycle the switch.



## Severity

ERROR

# SWCH-1004

## Message

```
timestamp, [SWCH-1004], sequence-number, , ERROR, system-name, Blade attach failed during recovery, disabling slot = slot-number
```

## Probable cause

A blade failed during failover or recovery.

## Recommended action

On a Core Switch 2/64 or SAN Director 2/128 switch, first run the `slotPowerOff` command and then run the `slotPowerOn` command.

On a SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, or SAN Switch 4/32 switch, reboot or power cycle the switch.

## Severity

ERROR

# SWCH-1005

## Message

```
timestamp, [SWCH-1005], sequence-number, , ERROR, system-name, Diag attach failed during recovery, disabling slot = slot-number
```

## Probable cause

The Diag blade attach failed during failover or recovery.

## Recommended action

On a Core Switch 2/64 or SAN Director 2/128 switch, run first the `slotPowerOff` and then the `slotPowerOn` commands.

On a SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, or SAN Switch 4/32 switch, reboot or power cycle the switch.

## Severity

ERROR

---

# System controller error messages

## SYSC-1001

### Message

```
timestamp, [SYSC-1001], sequence-number,, CRITICAL, system-name, Failed to  
runname-of-program-that-could-not-be-run-(string):system-internal-error-m  
essage-(string)
```

### Probable cause

During the boot sequence one of the programs would not run on the system.

### Recommended action

1. If the message is reported during a reboot after new firmware has been loaded, try reloading the firmware using the `firmwareDownload` command.
2. If the message persists, a conflict may exist between the two versions of firmware or the nonvolatile storage may be corrupted.
3. Run the `supportFtp` command as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

### Severity

CRITICAL

## SYSC-1002

### Message

```
timestamp, [SYSC-1002], sequence-number,, CRITICAL, system-name, Switch  
bring-up timed out
```

### Probable cause

The system timed out during a reboot or failover sequence, waiting for one or more programs to register with system services or to fail over to active status.

### Recommended action

The switch is in an inconsistent state, which can be corrected only by a reboot or power cycle. Before rebooting the chassis, record the firmware version on the switch (or CP) and run the `haDump` command. If this is a dual-CP switch, then gather the output from the CP in which this log message appeared.

### Severity

CRITICAL

---

# General system error messages

## SYSM-1001

### Message

```
timestamp, [SYSM-1001], sequence-number,, CRITICAL, system-name, No memory
```

### Probable cause

The switch ran out of system memory.

### Recommended action

1. Run the `memShow` command to view the switch memory usage.
2. Reboot or power cycle the switch.

### Severity

CRITICAL

## SYSM-1002

### Message

```
timestamp, [SYSM-1002], sequence-number,, INFO, system-name, number,  
Switch: switch-number
```

### Probable cause

A user executed either the `switchShutdown` or `switchReboot` command. All services were brought down for a logical switch.

### Recommended action

No action is required if the `switchShutdown` or `switchReboot` command was executed intentionally. If the `switchShutdown` command was run, you must run the `switchStart` command to restart traffic on the logical switch.

### Severity

INFO

## SYSM-1003

### Message

```
timestamp, [SYSM-1003], sequence-number,, INFO, system-name, number,  
Switch: start-reason
```

## Probable cause

The user executed the `switchStart` or `switchReboot` command. All services are brought back up after a temporary shutdown of that logical switch.

## Recommended action

No action is required if the `switchStart` or `switchReboot` command was executed intentionally. Because reinitializing a switch is a disruptive operation and can stop I/O traffic, you may have to stop and restart the traffic during this process.

## Severity

INFO

# SYSM-1004

## Message

```
timestamp, [SYSM-1004], sequence-number,, ERROR, system-name, Failed to  
retrieve current chassis configuration option, ret=%d
```

## Probable cause

A failure to read configuration data from the WWN card occurred.

## Recommended action

Verify that the WWN card is present and operational and that the affected CP is properly seated in its slot.

## Severity

ERROR

---

# RAS trace error messages

## TRCE-1001

## Message

```
timestamp, [TRCE-1001], sequence-number,, WARNING, system-name, Trace dump  
available optional-slot-indicating-on-which-slot-the-dump-occurs!  
(reason:Text-explanation-of-what-triggered-the-dump-(PANICDUMP-WATCHDOGEX  
PIRED-MANUAL-TRIGGER))
```

## Probable cause

Trace dump files were generated on the switch or the indicated slot. The reason field indicates the cause for generating the dump:

- `PANICDUMP` is generated by panic dump
- `WATCHDOGEXPIRED` is generated by hardware watchdog expiration

- *MANUAL* is generated by the `tracedump -n` command
- *TRIGGER* when triggered by a specific Message ID generated by critical RASLog message or RASLog message trigger setup using the `traceTrig` command

## Recommended action

1. Run the `supportFtp` and `traceFtp` commands as needed to set up automatic FTP transfers.
2. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# TRCE-1002

## Message

```
timestamp, [TRCE-1002], sequence-number,, INFO, system-name, Trace dump
optional-slot-indicating-on-which-slot-the-dump-occurs automatically
transferred to FTP address 'FTP-target-designated-by-user'.
```

## Probable cause

A trace dump occurred on the switch or the indicated slot and successfully transferred from the switch automatically.

## Recommended action

No action is required.

## Severity

INFO

# TRCE-1003

## Message

```
timestamp, [TRCE-1003], sequence-number,, ERROR, system-name, Trace dump
optional-slot-indicating-on-which-slot-the-dump-occurs was not
transferred due to FTP error.
```

## Probable cause

A trace dump was created on the switch or the indicated slot, but was not automatically transferred from the switch due to an FTP error, such as wrong FTP address, FTP site down, network down, and so on.

## Recommended action

1. Run the `supportFtp` command as needed to set up automatic FTP transfers.
2. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# TRCE-1004

## Message

```
timestamp, [TRCE-1004], sequence-number,, WARNING, system-name, Trace dump  
optional-slot-indicating-on-which-slot-the-dump-occurs was not  
transferred because trace auto-FTP disabled.
```

## Probable cause

Trace dump files was created on the switch or the indicated slot, but was not automatically transferred from the switch because auto-FTP is disabled.

## Recommended action

1. Run the `supportFtp` command as needed to set up automatic FTP transfers.
2. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# TRCE-1005

## Message

```
timestamp, [TRCE-1005], sequence-number,, ERROR, system-name, FTP  
Connectivity Test failed due to error.
```

## Probable cause

The connectivity test to the FTP host failed because of a wrong FTP address, an FTP site down, or the network being down, and so on.

## Recommended action

1. Run the `supportFtp` command as needed to set up automatic FTP transfers.
2. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

## TRCE-1006

### Message

```
timestamp, [TRCE-1006], sequence-number,, INFO, system-name, FTP  
Connectivity Test succeeded to FTP site 'FTP-target-configured-by-users.'
```

### Probable cause

A connectivity test to the FTP host succeeded.

### Recommended action

No action is required.

### Severity

INFO

## TRCE-1007

### Message

```
timestamp, [TRCE-1007], sequence-number,, ERROR, system-name, Notification  
of this CP has failed. Parameters temporarily out of synch with other CP.
```

### Probable cause

The active CP was unable to alert the standby CP of a change in trace status. This message is applicable only to the Core Switch 2/64 and SAN Director 2/128.

### Recommended action

1. This message is often transitory. Wait a few minutes and try the command again.
2. If the problem persists, run the `supportFtp` command as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

### Severity

ERROR

## TRCE-1008

### Message

```
timestamp, [TRCE-1008], sequence-number,, CRITICAL, system-name, Unable to  
load trace parameters.
```

### Probable cause

The active CP was unable to read stored trace parameters.

## Recommended action

1. Reboot the CP (dual-CP system) or restart the switch.
2. Run the `traceFtp` command to set up for automatic FTP transfers.
3. Run the `supportFtp` command as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.

## Severity

CRITICAL

# TRCE-100

## Message

```
timestamp, [TRCE-1009], sequence-number,, ERROR, system-name, Unable to  
alert active CP that a dump has occurred.
```

## Probable cause

The standby CP was unable to communicate trace information to the active CP. This message is applicable only to the Core Switch 2/64 and SAN Director 2/128.

## Recommended action

1. Run the `haShow` command to verify that the current CP is standby and the active CP is active.
2. If the message persists, run the `supportFtp` command as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# TRCE-1010

## Message

```
timestamp, [TRCE-1010], sequence-number,, ERROR, system-name, Traced fails  
to start
```

## Probable cause

The trace daemon (traced), used for transferring trace files, failed to start. The trace capability within the switch is unaffected.

## Recommended action

1. Reboot the CP (dual-CP system) or restart the switch.
2. Run the `traceFtp` command to set up for automatic FTP transfers.
3. If the message persists, run the `supportFtp` command as needed to set up automatic FTP transfers.
4. Run the `supportSave` command and contact your switch service provider.



## Severity

ERROR

# TRCE-1011

## Message

```
timestamp, [TRCE-1011], sequence-number,, INFO, system-name, Trace dump manually transferred to target 'optional-string-to-indicate-which-slot-the-dump-is-ftped-out.': result.
```

## Probable cause

A manual transfer of trace dump files occurred.

## Recommended action

No action is required.

## Severity

INFO

---

# Track change feature error messages

# TRCK-1001

## Message

```
timestamp, [TRCK-1001], sequence-number,, INFO, system-name, Successful login by user user.
```

## Probable cause

The track change feature recorded a successful login.

## Recommended action

No action is required.

## Severity

INFO

# TRCK-1002

## Message

```
timestamp, [TRCK-1002], sequence-number,, INFO, system-name, Unsuccessful  
login by user user.
```

## Probable cause

The track change feature recorded a failed login. This occurs if the user name or password is entered incorrectly. Normally, this message indicates a typing error by an authorized user. If this message occurs repeatedly, it may indicate an unauthorized user trying to gain access to a switch. When secure mode is enabled on the fabric, the IP address of a failed login is reported to the error log.

## Recommended action

No action is required.

## Severity

INFO

# TRCK-1003

## Message

```
timestamp, [TRCK-1003], sequence-number,, INFO, system-name, Logout by  
user user.
```

## Probable cause

The track change feature recorded a successful logout.

## Recommended action

No action is required.

## Severity

INFO

# TRCK-1004

## Message

```
timestamp, [TRCK-1004], sequence-number,, INFO, system-name, Config  
file change from task:task
```

## Probable cause

The track change feature recorded a configuration change for the switch.

The track change feature records any change to the configuration file in nonvolatile memory, including a `configDownload`. This message is not generated for a `configUpload`. All configuration changes occur through the PDM server, so the PDMIPC is the only task possible.

### Recommended action

No action is required. Run the `configShow` command to view the configuration file.

### Severity

INFO

## TRCK-1005

### Message

```
timestamp, [TRCK-1005], sequence-number, , INFO, system-name, Track-changes  
on
```

### Probable cause

The track change feature was enabled.

### Recommended action

No action is required. Run the `trackChangesSet 0` command if you want to disable the track change feature.

### Severity

INFO

## TRCK-1006

### Message

```
timestamp, [TRCK-1006], sequence-number, , INFO, system-name, Track-changes  
off
```

### Probable cause

The track change feature was disabled.

### Recommended action

No action is required. Run the `trackChangesSet 1` command if you want to enable the track changes feature.

### Severity

INFO

---

# Time service error messages

## TS-1001

### Message

```
timestamp, [TS-1001], sequence-number,, WARNING, system-name, NTP Query failed: error-code
```

### Probable cause

A Network Time Protocol (NTP) query to the configured external clock server failed.

Local clock time on the principal or primary FCS switch is used for fabric synchronization. This may be logged during temporary operational issues, such as IP network connection issues to the external clock server. If it does not recur, it can be ignored.

### Recommended action

Verify that the configured external clock server is available and functional. If that external clock server is not available, choose another.

### Severity

WARNING

## TS-1002

### Message

```
timestamp, [TS-1002], sequence-number,, WARNING, system-name, type-of-clock-server-used Clock Server used instead of type-of-clock-server-configured: locl: 0xcode remote: 0xcode
```

### Probable cause

The fabric time synchronization distributed from the principal or primary FCS switch was not sourced from the *type-of-clock-server-configured*. Instead, an alternate server was used, indicated by *type-of-clock-server-used*. The type of clock server used or configured may be either:

- *LOCL*, which is a local clock on the principal or primary FCS switch
- *External*, which is an external NTP server address configured

This may be logged during temporary operational issues, such as IP network connection issues to the external clock server, or if the fabric is configured for external time synchronization but the principal or primary FCS does not support the feature. If the message does not recur, it should be ignored.

### Recommended action

1. Run the `tsClockServer` command to verify that the principal or primary FCS switch has the clock server IP configured correctly.
2. Verify that this clock server is accessible to the switch and functional.

3. If the principal or primary FCS does not support the feature, either choose a different switch for the role or reset the clock server to LOCL.

## Severity

WARNING

# TS-1006

## Message

```
timestamp, [TS-1006], sequence-number,, INFO, system-name, message
```

## Probable cause

A time service event is occurring or failed. The *message* can be one of the following:

- Init failed. Time Service exiting  
Probable cause: Initialization error or Time Server exits.
- Synchronizing time of day clock  
Probable cause: Usually logged during temporary operational issues when the clock goes out of synchronization. For example, when a time update packet is missed due to fabric reconfiguration or role change of the principal or primary FCS switch. If the message does not recur, it should be ignored.
- Validating time update  
Probable cause: Usually logged during temporary operational issues when a time update packet cannot be validated in a secure fabric. For example, during fabric reconfiguration or role change of the primary FCS switch. If the message does not recur, it should be ignored.

## Recommended action

No action is required.

## Severity

INFO

---

# Unicast error messages

## UCST-1003

## Message

```
timestamp, [UCST-1003], sequence-number,, INFO, system-name, Duplicate  
Path to Domain domain-ID, Output Port = port-number, PDB pointer = 0xvalue
```

## Probable cause

Duplicate paths were reported to the specified domain from the specified output port. The path database (PDB) pointer is the address of the path database and provides debugging information.

## Recommended action

No action is required.

## Severity

INFO

# UCST-1007

## Message

```
timestamp, [UCST-1007], sequence-number,, CRITICAL, system-name,  
Inconsistent route detected: Port = port-number, should be port-number
```

## Probable cause

The switch detected an inconsistency in the routing database between the routing protocol and the hardware configuration. The first port number displayed is what the hardware has configured and the second port number displayed is what the protocol is using.

## Recommended action

1. Run the `switchDisable` command and then the `switchEnable` command to reset the routing database.
2. Run the `uRouteShow` command to display the new routing tables.

## Severity

CRITICAL

---

# UPATH error messages

## UPTH-1001

## Message

```
timestamp, [UPTH-1001], sequence-number,, WARNING, system-name, No minimum  
cost path in candidate list
```

## Probable cause

The specified switch is unreachable because no minimum cost path (FSPF UPATH) exists in the candidate list (domain ID list).

## Recommended action

No action is required. This ends the current SPF computation.

## Severity

WARNING

---

# User space software watchdog error messages

## USWD-1006

### Message

```
timestamp, [USWD-1006], sequence-number,, WARNING, system-name, uSWD:  
warning-message
```

### Probable cause

A warning state exists in the system. This is an internal-use-only message.

### Recommended action

No action is required.

### Severity

WARNING

---

# Web Tools error messages

## WEBD-1001

### Message

```
timestamp, [WEBD-1001], sequence-number,, WARNING, system-name, Missing or  
Invalid Certificate file -- HTTPS is configured to be enabled but could  
not be started.
```

### Probable cause

The SSL certificate file is either invalid or absent.

### Recommended action

1. Run the `configure` command to disable HTTPS. For more information on the `configure` command, refer to the *HP StorageWorks Fabric OS 4.x command reference guide*.
2. Install a valid key file and enable HTTPS again.

### Severity

WARNING

# WEBD-1002

## Message

```
timestamp, [WEBD-1002], sequence-number,, WARNING, system-name, Missing or  
Invalid Key file -- HTTPS is configured to be enabled but could not be  
started.
```

## Probable cause

The SSL key file is either invalid or absent.

## Recommended action

1. Run the `configure` command to disable HTTPS. For more information on the `configure` command, refer to the *HP StorageWorks Fabric OS 4.x command reference guide*.
2. Install a valid key file and enable HTTPS again.

## Severity

WARNING

# WEBD-1003

## Message

```
timestamp, [WEBD-1003], sequence-number,, INFO, system-name, HTTP/HTTPS  
interface disabled
```

## Probable cause

The HTTP/HTTPS interface is disabled. This is logged when HTTP/HTTPS is disabled through the `configure` command.

## Recommended action

Run the `configure` command to enable HTTP/HTTPS. For more information on the `configure` command, refer to the *HP StorageWorks Fabric OS 4.x command reference guide*.

## Severity

INFO

# WEBD-1004

## Message

```
timestamp, [WEBD-1004], sequence-number,, INFO, system-name, HTTP server  
will be restarted due to configuration change
```

## Probable cause

The HTTP server configuration changed.



## Recommended action

No action is required.

## Severity

INFO

# WEBD-1005

## Message

```
timestamp, [WEBD-1005], sequence-number,, WARNING, system-name, HTTP  
server will be restarted for logfile truncation
```

## Probable cause

The size of the HTTP logfile exceeds the maximum limit.

## Recommended action

No action is required.

## Severity

WARNING

# WEBD-1006

## Message

```
timestamp, [WEBD-1006], sequence-number,, INFO, system-name, HTTP server  
restarted due to logfile truncation
```

## Probable cause

The size of the HTTP logfile exceeds the maximum limit.

## Recommended action

No action is required.

## Severity

INFO

# WEBD-1007

## Message

```
timestamp, [WEBD-1007], sequence-number,, INFO, system-name, HTTP server  
will be restarted due to change of IP Address
```

## Probable cause

The IP address of the switch changed and the HTTP server was restarted.

## Recommended action

No action is required.

## Severity

INFO

---

# Zone library module error messages

## ZOLB-1001

### Message

```
timestamp, [ZOLB-1001], sequence-number,, ERROR, system-name, ZONELIB  
error-message
```

## Probable cause

An internal timeout occurred on the IPC between the name server (NS) and the zoning modules. This usually indicates that the system was busy.

## Recommended action

1. This message generates core dump files of the related modules (zoned, nsd, rcsd). Copy these core files using the `saveCore` command.
2. If the message persists, run the `supportFtp` command as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

---

# Zone module error messages

## ZONE-1002

### Message

```
timestamp, [ZONE-1002], sequence-number,, WARNING, system-name, WWN  
zoneTypeCheck or zoneGroupCheck warning(warning-string) at  
port(port-number)
```

## Probable cause

A zone filter or zone group check failure occurred.

The frame filter logic reported a failure when creating or adding zone groups during port login (PLOGI) trap processing. This message usually indicates problems when adding CAM entries before the filter setup.

## Recommended action

1. If the message persists, run the `supportFtp` command as needed to set up automatic FTP transfers.
2. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# ZONE-1003

## Message

```
timestamp, [ZONE-1003], sequence-number,, WARNING, system-name,  
zone(current-zone) contains (domain-ID, port-number) which does not exist.
```

## Probable cause

The port zone member that is targeted for the local switch contains a non-existent port. The effective zoning configuration (displayed in the error message) contains a port number that is out of range.

## Recommended action

Edit the zone database and change the port number to a viable value in the effective configuration.

## Severity

WARNING

# ZONE-1004

## Message

```
timestamp, [ZONE-1004], sequence-number,, INFO, system-name, port  
port-number enforcement changed to Session Based HARD Zoning.
```

## Probable cause

The zoning enforcement changed to session-based hard zoning.

When a device is zoned using both WWN in one zone and *domain, portarea* in another, it causes that port to change to session-based hard zoning.

In session-based zoning, the zone enforcement is checked by the software. In hardware-enforced zoning, zone or alias members are defined using *domain, portarea* exclusively or using WWNs exclusively; that is, using one method or the other to define all objects in the zoning database. If the devices on the port are defined by a mixture of port IDs and WWNs, the zone enforcement is session based. If the S\_ID list of the hardware-enforced zoning overflows (over the S\_ID limit), the hardware zone enforcement changes to session-based zoning.

## Recommended action

No action is required.

## Severity

INFO

# ZONE-1005

## Message

```
timestamp, [ZONE-1005], sequence-number,, INFO, system-name, HARD & SOFT  
zones(zone-name, zone-name) definitions overlap.
```

## Probable cause

A port is zoned with mixed devices (WWN and *domain, portarea*). During zoning database cross checking, the system detects that either:

- A port zone member is also listed as a member of a mixed zone
- A WWN zone member is also specified as a member of a mixed zone

Use hard zone enforcement whenever possible. Hard zones are more secure than session-based hard zones. Both types of zones trap a port login (PLOGI), but hard zones filter out the I/O frames that session-based hard zones do not.

## Recommended action

If hard zone enforcement is preferred, edit the zoning database to have the port zoned with devices defined as either WWN or defined as *domain, portarea*, but do not mix the methods used to define these zone members.

## Severity

INFO

# ZONE-1006

## Message

```
timestamp, [ZONE-1006], sequence-number,, WARNING, system-name, WARNING -  
WWN(WWN-number) in HARD PORT zone zone-name.
```

## Probable cause

One or more devices are zoned as WWN devices and also zoned as *domain, portarea* devices. The devices are used to specify zone members over separate zones.

## Recommended action

If hardware zoning enforcement is preferred, edit the zoning database to have the device zoned using only one specification type: either WWN or *domain, portarea*.

## Severity

WARNING

# ZONE-1007

## Message

```
timestamp, [ZONE-1007], sequence-number,, INFO, system-name,  
Ioctl(function) in (error-message) at port (port-number) returns code  
(error-string) and reason string (reason-string)
```

## Probable cause

Frame filter logic reported a failure during one of the IOCTL calls.

The IOCTL call from which the failure is reported is listed as part of the error message. This is usually a programming error when adding CAM entries before the filter setup.

## Recommended action

There are two ways to avoid this problem:

- Avoid having too many hosts zoned with a set of target devices at a single port.
- Avoid having too many zones directed at a single port group on the switch.

## Severity

INFO

# ZONE-1008

## Message

```
timestamp, [ZONE-1008], sequence-number,, WARNING, system-name, WARNING -  
port port-number Out of CAM entries
```

## Probable cause

The total number of entries of S\_ID CAM was above the limit while creating or adding a zone group. The maximum number of CAM entries allowed depends on the ASIC.

## Recommended action

If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

## Severity

WARNING

# ZONE-1010

## Message

```
timestamp, [ZONE-1010], sequence-number,, WARNING, system-name, WARNING -  
Duplicate entries in zone(zone-name) specification.
```

### Probable cause

Duplicate entries were detected in a zone object. A zone object member is specified twice in a given zone object. This message occurs only when enabling a zone configuration.

### Recommended action

Check the members of the zone and delete the duplicate member.

### Severity

WARNING

# ZONE-1012

## Message

```
timestamp, [ZONE-1012], sequence-number,, WARNING, system-name, WARNING -  
All ports are offline.
```

### Probable cause

All the ports in a zone are offline.

### Recommended action

Check the device connection.

### Severity

WARNING

# ZONE-1013

## Message

```
timestamp, [ZONE-1013], sequence-number,, WARNING, system-name, Quick Loop  
not supported.
```

### Probable cause

The QuickLoop feature is not supported in the current code release. If the QuickLoop zoning configuration is enabled on the switch, it is not supported.

### Recommended action

Edit the zone database to remove the QuickLoop zoning definition from the effective configuration.

## Severity

WARNING

# ZONE-1014

## Message

```
timestamp, [ZONE-1014], sequence-number,, ERROR, system-name, Missing  
required license - license-name.
```

## Probable cause

The required zoning license is missing.

## Recommended action

Install the zoning license using the `licenseAdd` command. Refer to your switch supplier to obtain a zoning license if you do not have one.

## Severity

ERROR

# ZONE-1015

## Message

```
timestamp, [ZONE-1015], sequence-number,, WARNING, system-name, Not owner  
of the current transaction transaction-ID
```

## Probable cause

A zoning change operation is not allowed because the zoning transaction is opened by another task. Indicates concurrent modification of the zone database by multiple administrators.

## Recommended action

Wait until the previous transaction is complete. Verify that only one administrator at a time is working with the zone database.

## Severity

WARNING

# ZONE-1017

## Message

```
timestamp, [ZONE-1017], sequence-number,, ERROR, system-name, FA  
Zone(zone-name) contains incorrect number of Initiator and Target devices
```

## Probable cause

The Fabric Assist (FA) zoning configuration has more than one initiator. The probable cause is incorrect entries in the FA zoning configuration.

## Recommended action

Edit the zone database to ensure that only one initiator is set for each FA zone configuration.

## Severity

ERROR

# ZONE-1018

## Message

```
timestamp, [ZONE-1018], sequence-number,, ERROR, system-name, Incorrect  
zoning enforcement type(zone-type) at port(port-number)
```

## Probable cause

An incorrect zoning enforcement type was reported on the specified port. This is a software error. A QuickLoop zone type (value = 4) and an uninitialized type (value = 0) are invalid. The valid zone type values are:

- Hard port zone (value = 1)
- Hard WWN zone (value = 2)
- Session based hard zoning (value = 3)
- FA zone (value = 5)

QuickLoop zones are not supported in Fabric OS v4.x.

## Recommended action

1. If the message persists, run the `supportFtp` command as needed to set up automatic FTP transfers.
2. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# ZONE-1019

## Message

```
timestamp, [ZONE-1019], sequence-number,, ERROR, system-name, Transaction  
Commit failed. Reason code reason-code (application-reason) -  
\"reason-string\"
```



## Probable cause

The reliable commit service (RCS) had a transmit error. RCS is a protocol used to transmit changes to the configuration database within a fabric.

## Recommended action

1. Often this message indicates a transitory problem. Wait a few minutes and retry the command.
2. Make sure that your changes to the zone database are not overwriting the work of another admin.
3. Run the `cfgTransShow` command to determine whether any outstanding transactions are running on the local switches.
4. If the message persists, run the `supportFtp` command as needed to set up automatic FTP transfers.
5. Run the `supportSave` command and contact your switch service provider.

## Severity

ERROR

# ZONE-1022

## Message

```
timestamp, [ZONE-1022], sequence-number,, INFO, system-name, The effective configuration has changed
```

## Probable cause

The effective zone configuration changed.

## Recommended action

Verify that this zone configuration change was intended. If the new effective zone configuration is correct, no action is necessary.

## Severity

INFO

# ZONE-1023

## Message

```
timestamp, [ZONE-1023], sequence-number,, INFO, system-name, Switch connected to port (port-number) is busy. Retry zone merge
```

## Probable cause

The switch is retrying the merge operation. This usually occurs if the switch on the other side of the port is busy.

## Recommended action

1. If the message persists, run the `supportFtp` command as needed to set up automatic FTP transfers.

2. Run the `supportSave` command and contact your switch service provider.

## Severity

INFO

# ZONE-1024

## Message

```
timestamp, [ZONE-1024], sequence-number,, INFO, system-name,  
information-message
```

## Probable cause

The `cfgSave` command ran successfully.

## Recommended action

No action is required.

## Severity

INFO

# ZONE-1026

## Message

```
timestamp, [ZONE-1026], sequence-number,, INFO, system-name, port  
port-number Out of CAM entries
```

## Probable cause

The total number of S\_ID entries while creating or adding a zone group exceeds the limit.

## Recommended action

If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

## Severity

INFO

# ZONE-1027

## Message

```
timestamp, [ZONE-1027], sequence-number,, ERROR, system-name, Zoning  
transaction aborted - error-reason
```

## Probable cause

The zoning transaction was aborted due to a variety of potential errors.

The *error-reason* values are:

- Zone Merge Received: The fabric is in the process of merging two zone databases.
- Zone Config update Received: The fabric is in the process of updating the zone database.
- Bad Zone Config: The new config is not viable.
- Zoning Operation failed: A zoning operation failed.
- Shell exited: The command shell exited.
- Unknown: An error was received for an unknown reason.
- User Command: A user aborted the current zoning transaction.
- Switch Shutting Down: The switch is currently shutting down.

## Recommended action

Many of the causes of this error message are transitory: for example, if two admins are working with the zoning database concurrently.

1. If you receive this error, wait a few minutes and try again.
2. Verify that no one else is currently modifying the zone database.

## Severity

ERROR

# ZONE-1028

## Message

```
timestamp, [ZONE-1028], sequence-number,, WARNING, system-name, Commit  
zone DB larger than supported - zone-db-size greater than max-zone-db-size
```

## Probable cause

The zone database size is greater than the limit allowed by the fabric.

The limit of the zone database size depends on the lowest-level switch in the fabric. Older switches have less memory and force a smaller zone database for the entire fabric.

## Recommended action

Edit the zone database to keep it within the allowable limit for the specific switches in your fabric. Refer to the *HP StorageWorks Fabric OS 4.x procedures user guide* for information on the zone database sizes supported for each switch.

## Severity

WARNING

# ZONE-1029

## Message

```
timestamp, [ZONE-1029], sequence-number,, WARNING, system-name, Restoring  
zone cfg from flash failed - bad config saved to config-file-name  
[return-code]
```

## Probable cause

The zone configuration restored from the flash was faulty.

## Recommended action

1. This error saves the bad zone configuration in the zoned core file directory. Run the `saveCore` command to save the file.
2. If the message persists, run the `supportFtp` command as needed to set up automatic FTP transfers.
3. Run the `supportSave` command and contact your switch service provider.

## Severity

WARNING

# ZONE-1030

## Message

```
timestamp, [ZONE-1030], sequence-number,, WARNING, system-name, Converting  
the zone db for PID format change failed
```

## Probable cause

The current zone database could not be converted to reflect the PID format change. Most likely this is caused by the size of the database.

## Recommended action

1. Change the PID format back to its original format.
2. Correct the zone database. Usually this involves reducing the size of the database.
3. Change the PID format back to the PID format you requested.

## Severity

WARNING

# Glossary

## **AL\_PA**

Arbitrated-loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop. Alternately, *arbitrated-loop parameters*.

## **alias**

A logical grouping of elements in a fabric. An alias is a collection of port numbers and connected devices that simplify the entry of port numbers and WWNs during zone creation.

## **ARB**

Arbitrative primitive signal. Applies only to an arbitrated-loop topology. Transmitted as the fill word by an L\_Port to indicate that the port is arbitrating access to the loop.

## **area number**

In Fabric OS v4.0 and later, ports on a switch are assigned a logical area number. Port area numbers can be viewed by issuing the `switchshow` command. They define the operative port for many Fabric OS commands; for example, area numbers can be used to define the ports within an alias or zone.

## **ASIC**

Application-specific integrated circuit.

## **authentication**

The process of verifying that an entity in a fabric, such as a switch, is what it claims to be. See also [digital certificate](#).

## **autocommit**

A feature of the `firmwaredownload` command. Enabled by default, `autocommit` commits new firmware to both partitions of a control processor.

## **autoreboot**

Refers to the `-b` option of the `firmwaredownload` command. Enabled by default.

## **backbone fabric**

An optional capability that enables scalable meta-SANs by allowing the networking of multiple FC routers, which connect to the backbone fabric via EB\_Port interfaces.

## **backup FCS switch**

Relates to the Secure Fabric OS feature. The backup fabric configuration server serves as a backup in case the primary FCS switch fails. See also [FCS switch](#), [primary FCS switch](#).

## **BB fabric**

A backbone fabric that connects FC Routers. The FC Routers communicate over the backbone fabric using FCRP (Fibre Channel Router Protocol).

## **BB\_Credit**

Buffer-to-buffer credit. The number of frames that can be transmitted to a directly connected recipient or within an arbitrated loop. Determined by the number of receive buffers available. See also [buffer-to-buffer flow control](#), [EE\\_Credit](#).

## **beacon**

A tool in which all of the port LEDs on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by a CLI command or through Advanced Web Tools.

## **BISR**

Built-in self-repair.

## **BIST**

Built-in self-test.

## **broadcast**

The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also [multicast](#).

## **buffer-to-buffer flow control**

Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop. See also [BB\\_Credit](#).

## **cascade**

Two or more interconnected Fibre Channel switches. See also [fabric](#), [ISL](#).

## **CHAP**

Challenge-Handshake Authentication Protocol. Allows remote servers and clients to securely exchange authentication credentials. Both the server and client are configured with the same shared secret. See also [DH-CHAP](#).

## **chassis**

The metal frame in which the switch and switch components are mounted.

## **Class 1 service**

The class of frame-switching service for a dedicated connection between two communicating ports (also called *connection-oriented service*). Includes acknowledgement of frame delivery or nondelivery.

## **Class 2 service**

A connectionless class of frame-switching service that includes acknowledgement of frame delivery or nondelivery.

## **Class 3 service**

A connectionless class of frame-switching service that does not include acknowledgement of frame delivery or nondelivery. Can be used to provide a multicast connection between the frame originator and recipients, with acknowledgement of frame delivery or nondelivery.

## **Class 4 service**

A connection-oriented service that allows fractional parts of the bandwidth to be used in a virtual circuit.

## **Class 6 service**

A connection-oriented multicast service geared toward video broadcasts between a central server and clients.

## Class F service

The class of frame-switching service for a direct connection between two switches, allowing communication of control traffic between the E\_Ports. Includes acknowledgement of data delivery or nondelivery.

## class of service

A specified set of delivery characteristics and attributes for frame delivery.

## CLI

Command line interface. An interface that depends entirely on the use of commands, such as through telnet or SNMP, and does not involve a GUI. *See also* [SNMP](#).

## client

An entity that, using its common transport (CT), makes requests of a server.

## community (SNMP)

A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. *See also* [SNMP](#).

## compact flash

Flash or temporary memory that is used in a manner similar to hard disk storage. It is connected to a bridging component that connects to the PCI bus of the processor. Not visible within the processor's memory space.

## configuration

1. A set of parameters that can be modified to fine-tune the operation of a switch. Run the `configshow` command to view the current configuration of your switch.
2. In Zoning, a zoning element that contains a set of zones. The Configuration is the highest-level zoning element and is used to enable or disable a set of zones on the fabric. *See also* [zone configuration](#).

## congestion

The realization of the potential of oversubscription. A congested link is one on which multiple devices are contending for bandwidth.

## core PID

Core switch port identifier. The core PID must be set for v3.1 and earlier switches included in a fabric of v4.1 switches. This parameter is located in the `configure` command of firmware versions v3.1 and earlier. All v4.1 switches and later use the core PID format by default; this parameter is not present in the `configure` command for these switches. *See also* [PID](#).

## CSCN

Common services connection framework.

## defined zone configuration

The set of all zone objects defined in the fabric. Can include multiple zone configurations. *See also* [enabled zone configuration](#), [zone configuration](#).

## deskew

Related to the Trunking feature. The time difference between traffic traveling over each intersite link (ISL) other than the shortest ISL in the group and traffic traveling over that shortest ISL. The deskew number corresponds to nanoseconds divided by 10. The firmware automatically sets the minimum deskew value of the shortest ISL to 15.

## DH-CHAP

Diffie-Hellman Challenge-Handshake Authentication Protocol. An implementation of CHAP using Diffie-Hellman encryption. See also [CHAP](#).

## digital certificate

An electronic document issued by a certificate authority (CA) to an entity, containing the public key and identity of the entity. Entities in a secure fabric are authenticated based on these certificates. See also [authentication](#), [public key](#), [PKI](#), [PKI certification utility](#).

## director

An HP StorageWorks Core Switch 2/64, or SAN Director 2/128.

## domain ID

A unique identifier for all switches in a fabric, used in routing frames. Usually automatically assigned by the principal switch but can be assigned manually. The domain ID for an HP StorageWorks switch can be any integer between 1 and 239.

## E\_Port

Expansion port. A standard Fibre Channel mechanism that enables switches to network with each other, creating an ISL. See also [ISL](#).

## edge fabric

A Fibre Channel fabric connected to an FC router via an EX\_Port (where hosts and storage are attached in a meta-SAN).

## EE\_Credit

End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage frame exchange across the fabric, between source and destination. See also [BB\\_Credit](#), [Class 1 service](#), [Class 2 service](#).

## ELS

Fibre Channel - Extended Link Services Frame.

## EM

Environmental monitor. Monitors FRUs and reports failures.

## enabled zone configuration

The currently enabled configuration of zones. Only one configuration can be enabled at a time. See also [defined zone configuration](#), [zone configuration](#).

## error

As applied to the Fibre Channel industry, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors).

## Ethernet

Popular protocols for LANs.

## EX\_Port

A type of E\_Port that connects an FC router to an edge fabric. EX\_Ports limit the scope of fabric services, but provide device connectivity using FC-NAT.



## **exchange**

The highest-level Fibre Channel mechanism used for communication between N\_Ports. Composed of one or more related sequences, it can work in either one or both directions.

## **fabric**

A collection of Fibre Channel switches and devices, such as hosts and storage. Also referred to as a *switched fabric*. See also [cascade](#), [SAN](#), [topology](#).

## **Fabric Manager**

An optionally licensed software feature. Fabric Manager is a GUI that allows for fabric-wide administration and management. Switches can be treated as groups, and actions such as firmware downloads can be performed simultaneously.

## **fabric name**

The unique identifier assigned to a fabric and communicated during login and port discovery.

## **fabric port count**

The number of ports available for connection by nodes in a fabric.

## **Fabric Watch**

A licensed software feature. Fabric Watch can be accessed through either the command line or Advanced Web Tools, and provides the ability to set thresholds for monitoring fabric conditions.

## **failover**

The Core Switch 2/64 process of one CP passing active status to another CP. A failover is nondisruptive.

## **FC router**

A platform running the HP StorageWorks Fibre Channel Routing Service that enables two or more fabrics to share resources (such as hosts or storage devices) without merging those fabrics; the FCIP tunneling service for Fibre Channel over IP; or iSCSI gateway service (future capability) for iSCSI to Fibre Channel bridging. All three services can be run simultaneously.

## **FCIP**

Fibre Channel over IP.

## **FCS switch**

Relates to the HP StorageWorks Secure Fabric OS feature. One or more designated switches that store and manage security parameters and configuration data for all switches in the fabric. They also act as a set of backup switches to the primary FCS switch. See also [backbone fabric](#), [primary FCS switch](#).

## **FC-SW-2**

The second-generation Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches to create a multswitch Fibre Channel fabric.

## **FDDI**

Fibre Distributed Data Interface. An ANSI architecture for a metropolitan area network (MAN); a network based on the use of fiber-optic cable to transmit data at 100 Mbps

## **FDMI**

Fabric-Device Management Interface. FDMI is a database service provided by the fabric for Nx\_Ports. The primary use is by HBA devices that register information about themselves and their ports.

**FFFFF5**

Well-known Fibre Channel address for a Class 6 multicast server.

**FFFFF6**

Well-known Fibre Channel address for a clock synchronization server.

**FFFFF7**

Well-known Fibre Channel address for a security key distribution server.

**FFFFF8**

Well-known Fibre Channel address for an alias server.

**FFFFF9**

Well-known Fibre Channel address for a QoS facilitator.

**FFFFFA**

Well-known Fibre Channel address for a management server.

**FFFFFB**

Well-known Fibre Channel address for a time server.

**FFFFFC**

Well-known Fibre Channel address for a directory server.

**FFFFFD**

Well-known Fibre Channel address for a fabric controller.

**FFFFFE**

Well-known Fibre Channel address for a fabric F\_Port.

**FFFFF**

Well-known Fibre Channel address for a broadcast alias ID.

**Fibre Channel**

The primary protocol used for building SANs to transmit data between servers, switches, and storage devices. Unlike IP and Ethernet, Fibre Channel was designed to support the needs of storage devices of all types. It is a high-speed, serial, bidirectional, topology-independent, multiprotocol, and highly scalable interconnection between computers, peripherals, and networks.

**Fibre Channel transport**

A protocol service that supports communication between Fibre Channel service providers.

**FID**

Fabric ID. Unique identifier of a fabric in a meta-SAN.

**FIFO**

First in, first out. Refers to a data buffer that follows the first in, first out rule.

**fill word**

An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the Fibre Channel link active.

## **firmware**

The basic operating system provided with the hardware.

## **FL\_Port**

Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated-loop capabilities. Can be used to connect an NL\_Port to a switch. See also [Fx\\_Port](#).

## **flash**

Programmable nonvolatile random access memory (NVRAM); memory that retains its contents without power.

## **FLOGI**

Fabric login. The process by which an N\_Port determines whether a fabric is present and if so, exchanges service parameters with it. See also [PLOGI](#).

## **frame**

The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, optional headers, data payload, cyclic redundancy check (CRC), and end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements and so forth) and data frames.

## **frame relay**

A protocol that uses logical channels, as used in X.25. Provides very little error-checking ability. Discards frames that arrive with errors. Allows a certain level of bandwidth between two locations (known as a *committed information rate* (CIR) to be guaranteed by service provider. If CIR is exceeded for short periods (known as *bursts*), the network accommodates the extra data, if spare capacity is available. Frame relay is therefore known as *bandwidth on demand*.

## **FRU**

Field-replaceable unit. A component that can be replaced onsite.

## **FSPF**

Fabric shortest path first. The HP StorageWorks routing protocol for Fibre Channel switches.

## **FSS**

Fabric OS state synchronization. The FSS service is related to high availability (HA). The primary function of FSS is to deliver state update messages from active components to their peer standby components. FSS determines whether fabric elements are synchronized (and thus FSS compliant).

## **FTP**

File Transfer Protocol.

## **full fabric**

The HP StorageWorks software license that allows multiple E\_Ports on a switch, making it possible to create multiple ISL links.

## **full duplex**

A mode of communication that allows the same port to simultaneously transmit and receive frames. See also [half duplex](#).

## **Fx\_Port**

A fabric port that can operate as either an F\_Port or FL\_Port. See also [FL\\_Port](#).

## **G\_Port**

Generic port. A port that can operate as either an E\_Port or an F\_Port. A port is defined as a G\_Port when it is not yet connected or has not yet assumed a specific function in the fabric.

## **gateway**

Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can connect a Fibre Channel link to an ATM connection.

## **GBIC**

Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical-level transport for Fibre Channel and gigabit Ethernet.

## **Gbps**

Gigabits per second (1,062,500,000 bits/second). Also expressed as *Gbps*.

## **GBps**

Gigabytes per second (1,062,500,000 bytes/second). Also expressed as *GBps*.

## **GLM**

Gigabit Link Module. A semitransparent transceiver that incorporates serializing and deserializing functions.

## **GMT**

Greenwich Mean Time. An international time zone. Also called *UTC*.

## **GUI**

A graphic user interface, such as HP StorageWorks Advanced Web Tools arbitrated-loop topology and HP StorageWorks Fabric Manager.

## **HA**

High availability. A set of features in HP StorageWorks switches that provides maximum reliability and nondisruptive replacement of key hardware and software modules.

## **half duplex**

A mode of communication that allows a port to either transmit or receive frames at any time except simultaneously (with the exception of link control frames, which can be transmitted at any time). See also [full duplex](#).

## **hard address**

The AL\_PA that an NL\_Port attempts to acquire during loop initialization.

## **Hardware Translative Mode**

A method for achieving address translation. There are two hardware translative modes available to a QuickLoop enabled switch: *Standard Translative Mode* and *QuickLoop Mode*.

## **HBA**

Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

## **hop count**

The number of ISLs a frame must traverse to get from its source to its destination. See also [ISL](#).

## **host**

A computer system that provides end users with services like computation and storage access.

**hot swappable**

A component that can be replaced under power.

**HTTP**

Hypertext Transfer Protocol. The standard TCP/IP transfer protocol used on the World Wide Web.

**hub**

A Fibre Channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

**ICT**

Intracircuit test.

**ID\_ID**

Insistent domain ID. A parameter of the `configure` command in the HP StorageWorks Fabric OS.

**Insistent Domain ID Mode**

Sets the domain ID of a switch as insistent, so that it remains the same over reboots, power cycles, failovers, and fabric reconfigurations.

**integrated fabric**

The fabric created by an HP StorageWorks SAN Switch Integrated/64, consisting of six HP StorageWorks 1 GB switches cabled together and configured to handle traffic seamlessly as a group.

**IOCTL**

I/O control.

**iSCSI**

Internet Small Computer Systems Interface. A protocol that defines the processes for transferring block storage applications over TCP/IP networks by encapsulating SCSI commands into TCP and transporting them over the network via IP.

**iSCSI Gateway Service**

The HP StorageWorks multiprotocol SAN routing service that maps the FCP protocol to the IP transport. This service projects iSCSI hosts onto the backbone fabric of a gateway switch.

**ISL**

Interswitch link. A Fibre Channel link from the E\_Port of one switch to the E\_Port of another. See also [cascade](#), [E\\_Port](#).

**ISP**

Internet service provider.

**JBOD**

Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also [RAID](#).

**jitter**

A deviation in timing for a bit stream as it flows through a physical medium.

## key

A string of data (usually a numeric value) shared between two entities and used to control a cryptographic algorithm. Usually selected from a large pool of possible keys to make unauthorized identification of the key difficult. See *also* [key pair](#).

## key pair

In public key cryptography, a pair of keys consisting of an entity's public and private key. The public key can be publicized, but the private key must be kept secret.

## L\_Port

Loop port. A node port (NL\_Port) or fabric port (FL\_Port) that has arbitrated-loop capabilities. An L\_Port can be in either Fabric Mode or Loop Mode.

## LAN

Local area network. A network in which transmissions typically take place over less than 5 kilometers (3.4 miles).

## latency

The time required to transmit a frame. Together, latency and bandwidth define the speed and capacity of a link or system.

## LED

Light-emitting diode. An electronic indicator that shows the status of elements on a switch.

## login server

The unit that responds to login requests.

## Loop Mode

One of two possible modes for an L\_Port, in which the L\_Port is in an arbitrated loop, using loop protocol. An L\_Port in Loop Mode can also be in *Participating Mode* or *Nonparticipating Mode*.

## LSAN

Logical storage area network. An LSAN enables device and storage connectivity that spans two or more fabrics. The path between devices in an LSAN can be local to a fabric or cross one or more FC routers and one or more backbone fabrics.

## LSAN zone

The mechanism by which LSANs are administered. An FC router attached to two fabrics listens for the creation of matching LSAN zones on both fabrics. If this occurs, it creates phantom domains and FC-NAT entries as appropriate, and inserts entries for them into the name servers on the fabrics. LSAN zones are compatible with all standard zoning mechanisms.

## MALLOC

Memory allocation. Usually relevant to buffer credits.

## meta-SAN

The collection of all devices, switches, edge and backbone fabrics, LSANs, and FC routers that make up a physically connected but logically partitioned storage network. LSANs span between edge fabrics using FC routers. In a data network, this would simply be called *the network*. However, an additional term is required to specify the difference between a single-fabric network (**SAN**), a multifabric network without cross-fabric connectivity (*dual-redundant fabric SAN*), and a multifabric network with connectivity (*meta-SAN*). See *also* [SAN](#).

## **MIB**

Management Information Base. An SNMP structure that helps with device management, providing configuration and device information.

## **MS**

Management Server. The Management Server allows a SAN management application to retrieve information and administer the fabric and interconnected elements, such as switches, servers, and storage devices. The MS is located at the Fibre Channel well-known address `FFFFFFAh`.

## **MTBF**

Mean time between failures. An expression of time, indicating the longevity of a device.

## **multicast**

The transmission of data from a single source to multiple specified N\_Ports—as opposed to all the ports on the network. See also [broadcast](#).

## **multimode**

A fiber optic cabling specification that allows up to 500 meters between devices.

## **N\_Port**

Node port. A port on a node that can connect to a Fibre Channel port or to another N\_Port in a point-to-point connection. See also [NL\\_Port](#), [Nx\\_Port](#).

## **Name Server**

Simple Name Server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also called *directory service*.

## **NAS**

Network-attached storage. A disk array connected to a controller that gives access through a LAN.

## **NIC**

Network interconnect card.

## **NL\_Port**

Node loop port. A node port that has arbitrated-loop capabilities. Connects an equipment port to the fabric in a loop configuration through an FL\_Port. See also [N\\_Port](#), [Nx\\_Port](#).

## **node**

A Fibre Channel device that contains an N\_Port or NL\_Port.

## **node count**

The number of nodes attached to a fabric.

## **node name**

The unique identifier for a node, communicated during login and port discovery.

## **NR\_Port**

A normal E\_Port that connects an FC Router to a backbone fabric.

## NS

Name Server. The service provided by a fabric switch that stores names, addresses, and attributes related to Fibre Channel objects. Can cache information for up to 15 minutes. Also known as *Simple Name Server* or as a *directory service*. See also [Simple Name Server \(SNS\)](#).

## Nx\_Port

A node port that can operate as either an N\_Port or NL\_Port.

## oversubscription

A situation in which more nodes could potentially contend for a resource than the resource could simultaneously support (typically an ISL). Oversubscription could be a desirable attribute in fabric topology, as long as it does not produce unacceptable levels of congestion.

## OX\_ID

Originator ID or exchange ID. Refers to the exchange ID assigned by the originator port.

## payload

A Fibre Channel frame has a header and a payload. The payload contains the information being transported by the frame; it is determined by the higher-level service or FC\_4 upper-level protocol. There are many different payload formats, based on protocol.

## PBC

Port bypass circuit. A circuit in hubs or a disk enclosure to open or close a loop to add or remove nodes.

## PCBA

Printed circuit board assembly.

## PCM

Pulse-code modulation. A standard method of encoding analog audio signals in digital form.

## Performance Monitoring

An HP StorageWorks switch feature that monitors port traffic and includes frame counters, SCSI read monitors, SCSI write monitors, and other types of monitors.

## phantom device

A device that is not physically in an arbitrated-loop but is logically included through the use of a phantom address.

## phantom domain

See [xlate domain](#).

## PID

Port identifier. See also [core PID](#).

## PKI

Public key infrastructure. An infrastructure that is based on public key cryptography and certificate authority (CA) and that uses digital certificates. See also [digital certificate](#).

## PKI certification utility

Public key infrastructure certification utility. A utility that makes it possible to collect certificate requests from switches and to load certificates to switches. See also [digital certificate](#), [PKI](#).



## **PLOGI**

Port login. The port-to-port login process by which initiators establish sessions with targets. See *also* [FLOGI](#).

### **port**

In an HP StorageWorks switch environment, an SFP or GBIC receptacle on a switch to which an optic cable for another device is attached.

### **port address**

In Fibre Channel technology, the port address is defined in hexadecimal. In the HP StorageWorks Fabric OS, a port address can be defined by a domain and port number combination or by area number. In an ESCON Director, an address that specifies port connectivity parameters and assigns link addresses for attached channels and control units.

### **port name**

A user-defined alphanumeric name for a port.

### **port swapping**

The ability to redirect a failed port to another port. This feature is available in Fabric OS v4.1.0 and later.

### **port\_name**

The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

## **POST**

Power-on self-test. A series of tests run by a switch after it is turned on.

### **primary FCS switch**

Relevant to the HP StorageWorks Secure Fabric OS feature. The primary fabric configuration server switch actively manages security and configurations for all switches in the fabric. See *also* [backbone fabric](#), [FCS switch](#).

### **principal switch**

The first switch to boot up in a fabric. Ensures unique domain IDs among roles.

### **private device**

A device that supports arbitrated-loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

### **private key**

The secret half of a key pair. See *also* [key](#), [key pair](#).

### **private loop**

An arbitrated loop that does not include a participating FL\_Port.

### **private loop device**

A device that supports a loop and can understand 8-bit addresses but does not log in to the fabric.

### **private NL\_Port**

An NL\_Port that communicates only with other private NL\_Ports in the same loop and does not log in to the fabric.

## **protocol**

A defined method and set of standards for communication. Determines the type of error-checking, the data-compression method, how sending devices indicate an end of message, and how receiving devices indicate receipt of a message.

**pstate**

Port State Machine.

**public device**

A device that supports arbitrated-loop protocol, can interpret 8-bit addresses, and can log in to the fabric.

**public key**

The public half of a key pair. *See also* [key](#), [key pair](#).

**queue**

A mechanism for each AL\_PA address that allows for the collection of frames prior to sending them to the loop.

**QuickLoop**

An HP StorageWorks software product that allows multiple ports on a switch to create a logical loop. Devices connected via QuickLoop appear to each other as if they are on the same arbitrated loop.

**QuickLoop Mode**

Allows initiator devices to communicate with private or public devices that are not in the same loop.

**R\_RDY**

Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

**radius**

The greatest distance between any edge switch and the center of a fabric. A low-radius network is better than a high-radius network.

**RAID**

Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. *See also* [JBOD](#).

**RCS**

Reliable Commit Service.

**RCS\_SFC**

RCS Stage Fabric Config.

**RLS**

Read Link Status.

**route**

As applied to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. *See also* [FSPF](#).

**routing**

The assignment of frames to specific switch ports, according to frame destination.

**RR\_TOV**

Resource recovery timeout value. The minimum time a target device in a loop waits after a LIP before logging out a SCSI initiator.

## **RSCN**

Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes. The fabric controller issues RSCN requests to N\_Ports and NL\_Ports, but only if they have registered to be notified of state changes in other N\_Ports and NL\_Ports. This registration is performed through the State Change Registration (SCR) Extended Link Service. An N\_Port or NL\_Port can issue an RSCN to the fabric controller without having completed SCR with the fabric controller.

## **RTWR**

Reliable transport with response. May appear as a task in `portlogdump` command output.

## **RW**

Read/write. Refers to access rights.

## **RX**

Receiving frames.

## **SAN**

Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also [fabric](#).

## **SCC**

SC connector. A fiber-optic cable connector that uses a push-pull latching mechanism similar to common audio and video cables. For bidirectional transmissions, two fiber cables and two SC connectors (dual SC) are generally used. SC is specified by the TIA as FOCIS-3.

## **SCN**

State change notification. Used for internal state change notifications, not external changes. This is the switch logging when the port is online or is an Fx\_Port, not what is sent from the switch to the Nx\_Ports.

## **SCR**

State change registration. Extended Link Service (ELS) requests the fabric controller to add the N\_Port or NL\_Port to the list of N\_Ports and NL\_Ports registered to receive the Registered State Change Notification (RSCN) Extended Link Service.

## **SCSI**

Small Computer Systems Interface. A parallel bus architecture and a protocol for transmitting large data blocks a distance of 15 to 25 meters.

## **SCSI-2**

An updated version of the SCSI bus architecture.

## **SCSI-3**

A SCSI standard that defines transmission of SCSI protocol data over different kinds of links.

## **SDRAM**

The main memory for a switch.

## **sectelnet**

A protocol similar to telnet but with encrypted passwords for increased security.

## **Secure Fabric OS**

An optionally licensed HP StorageWorks feature that provides advanced, centralized security for a fabric.

## **security policy**

Rules that determine how security is implemented in a fabric. Security policies can be customized through HP StorageWorks Secure Fabric OS or HP StorageWorks Fabric Manager.

## **server**

A computer that processes end-user applications or requests.

## **SES**

SCSI Enclosure Services. A subset of the SCSI protocol that monitors temperature, power, and fan status for enclosed devices.

## **SFP**

Small-form-factor pluggable. A transceiver used on 2 GBps switches that replaces the GBIC.

## **Simple Name Server (SNS)**

A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also called *directory service* or *name server*.

## **SLAP**

Switch Link Authentication Protocol.

## **SLP**

Service Location Protocol.

## **SNMP**

Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also [community \(SNMP\)](#).

## **SNS**

Simple Name Server.

## **SOF**

Start of frame. A group of ordered sets that marks the beginning of a frame and indicates the class of service that the frame uses.

## **soft zone**

A zone consisting of zone members that are made visible to each other through client service requests. Typically, soft zones contain zone members that are visible to devices using Name Server exposure of zone members. The fabric does not enforce a soft zone. Note that well-known addresses are implicitly included in every zone.

## **SSH**

Secure shell. Used starting in HP StorageWorks Fabric OS v4.1 to support encrypted telnet sessions to the switch. SSH encrypts all messages, including the client sending the password at login.

## **SSL**

Secure sockets layer.

## **Standard Translative Mode**

Allows public devices to communicate with private devices that are directly connected to the fabric.

**striping**

A RAID technique for writing a file to multiple disks on a block-by-block basis, with or without parity. See also [RAID](#).

**switch**

A fabric device that provides bandwidth and high-speed routing of data via link-level addressing.

**switch name**

The arbitrary name assigned to a switch.

**switch port**

A port on a switch. Switch ports can be E\_Ports, F\_Ports, or FL\_Ports.

**syslog**

Syslog daemon, that is used to forward error messages.

**target**

A storage device on a Fibre Channel network.

**TC**

Track changes.

**TCP/IP**

Transmission Control Protocol Internet Protocol.

**telnet**

A virtual terminal emulation used with TCP/IP. *Telnet* is sometimes used as a synonym for the HP StorageWorks Fabric OS CLI.

**throughput**

The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also [BB fabric](#).

**Time Server**

A Fibre Channel service that allows for the management of all timers.

**topology**

As applied to Fibre Channel technology, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point to point, which is a direct link between two communication ports.
- Switched fabric; multiple n\_ports linked to a switch by F\_Ports.
- Arbitrated loop; multiple NL\_Ports connected in a loop.

**track changes**

An HP StorageWorks Fabric OS feature that can be enabled to report specific activities (for example, logins, logouts, and configuration task changes). The output from the track-changes feature is dumped to the error log for the switch.

**transceiver**

A device that converts one form of signaling to another for transmission and reception; in fiber optics, optical to electrical.

**translate domain**

See [xlate domain](#).

**Translative Mode**

A mode in which private devices can communicate with public devices across the fabric.

**transmission character**

A 10-bit character encoded according to the rules of the 8b/10b algorithm.

**transmission word**

A group of four transmission characters.

**trap (SNMP)**

The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also [SNMP](#).

**trunking**

In Fibre Channel technology, a feature that enables distribution of traffic over the combined bandwidth of up to four ISLs between adjacent switches, while preserving in-order delivery.

**trunking group**

A set of up to four trunked ISLs.

**trunking ports**

The ports in a set of trunked ISLs.

**TS**

Time Server.

**tunneling**

A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network but are connected by a different type of network.

**TX**

Transmit.

**U\_Port**

Universal port. A switch port that can operate as a G\_Port, E\_Port, F\_Port, or FL\_Port. A port is defined as a U\_Port when it is not connected or has not yet assumed a specific function in the fabric.

**WAN**

Wide area network.

**WAN\_TOV**

Wide area network timeout value.

**well-known address**

With regard to Fibre Channel technology, a logical address defined by Fibre Channel standards as assigned to a specific function and stored on the switch.

**workstation**

A computer used to access and manage the fabric. Also called a *management station* or *host*.

**WWN**

World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

**xlate domain**

Translate domain. A router virtual domain that represents an entire fabric. Device connectivity can be achieved from one fabric to another, over the router and through this virtual domain, without merging the two fabrics. Also called a *phantom domain*.

**zone**

A set of devices and hosts attached to the same fabric and configured as being in the same segment. Devices and hosts within the same zone have access to others in the zone but are not visible to any outside the zone.

**zone configuration**

A specified set of zones. Enabling a configuration enables all zones in that configuration. See also [defined zone configuration](#), [enabled zone configuration](#).

**zoning**

A feature in fabric switches or hubs that allows segmentation of a node by physical port, name, or address.





# Index

## A

- audit field [30](#)
- AUTH-1001 [47](#)
- AUTH-1002 [47](#)
- AUTH-1003 [48](#)
- AUTH-1004 [48](#)
- AUTH-1005 [48](#)
- AUTH-1006 [49](#)
- AUTH-1007 [49](#)
- AUTH-1008 [50](#)
- AUTH-1010 [50](#)
- AUTH-1011 [50](#)
- AUTH-1012 [51](#)
- AUTH-1013 [51](#)
- AUTH-1014 [52](#)
- AUTH-1017 [52](#)
- AUTH-1018 [53](#)
- AUTH-1020 [53](#)
- AUTH-1022 [54](#)
- AUTH-1023 [54](#)
- AUTH-1025 [55](#)
- AUTH-1027 [55](#)
- AUTH-1028 [56](#)
- AUTH-1029 [56](#)
- AUTH-1030 [57](#)
- AUTH-1031 [57](#)
- AUTH-1032 [58](#)
- AUTH-1033 [58](#)
- AUTH-1034 [59](#)
- AUTH-1035 [59](#)
- AUTH-1036 [60](#)
- AUTH-1037 [60](#)
- AUTH-1038 [61](#)
- authorized reseller, HP [21](#)

## B

- BL-1001 [62](#)
- BL-1002 [62](#)
- BL-1003 [63](#)
- BL-1004 [63](#)
- BL-1006 [64](#)
- BL-1007 [64](#)
- BL-1008 [65](#)
- BL-1009 [65](#)
- BL-1010 [66](#)
- BL-1011 [66](#)
- BL-1012 [67](#)
- BL-1013 [67](#)
- BL-1014 [68](#)
- BL-1015 [68](#)
- BL-1016 [69](#)

- BLL-1000 [69](#)

## C

- CER-1001 [71](#)
- changes for this release of the Fabric OS [23](#)
- clearing the system message log [37](#)
- conventions
  - document [20](#)
  - text symbols [20](#)
- core dump files [31](#)

## D

- document
  - conventions [20](#)
  - related documentation [19](#)
- dual-CP systems [31](#)
- dumping the system messages [36](#)

## E

- EM-1001 [71](#)
- EM-1002 [72](#)
- EM-1003 [72](#)
- EM-1004 [73](#)
- EM-1005 [74](#)
- EM-1006 [75](#)
- EM-1007 [75](#)
- EM-1008 [76](#)
- EM-1009 [76](#)
- EM-1010 [77](#)
- EM-1011 [77](#)
- EM-1012 [77](#)
- EM-1013 [78](#)
- EM-1014 [79](#)
- EM-1015 [80](#)
- EM-1016 [80](#)
- EM-1017 [80](#)
- EM-1028 [81](#)
- EM-1029 [82](#)
- EM-1031 [82](#)
- EM-1033 [83](#)
- EM-1034 [83](#)
- EM-1036 [84](#)
- EM-1041 [85](#)
- EM-1042 [86](#)
- EM-1043 [86](#)
- EM-1044 [87](#)
- EM-1045 [87](#)
- EM-1046 [88](#)
- EM-1047 [88](#)
- EM-1048 [89](#)
- EM-1049 [89](#)

EM-1050 [90](#)  
EM-1051 [91](#)  
EM-1052 [91](#)  
EM-1053 [92](#)  
EM-1055 [93](#)  
EM-1056 [93](#)  
EVMD-1001 [94](#)  
example system message [34](#)

## F

FABR-1001 [94](#)  
FABR-1002 [95](#)  
FABR-1003 [95](#)  
FABR-1004 [96](#)  
FABR-1005 [96](#)  
FABR-1006 [97](#)  
FABR-1007 [97](#)  
FABR-1008 [98](#)  
FABR-1009 [98](#)  
FABR-1010 [99](#)  
FABR-1011 [99](#)  
FABR-1012 [99](#)  
FABR-1013 [100](#)  
FABR-1014 [100](#)  
FABR-1015 [101](#)  
FABR-1016 [101](#)  
FABR-1017 [101](#)  
FABR-1018 [101](#)  
FABR-1019 [102](#)  
FABR-1020 [102](#)  
FABR-1021 [103](#)  
FABR-1022 [103](#)  
FABR-1023 [103](#)  
FABR-1024 [104](#)  
FABR-1029 [104](#)  
FABS-1001 [105](#)  
FABS-1002 [105](#)  
FABS-1004 [106](#)  
FABS-1005 [106](#)  
FABS-1006 [107](#)  
FABS-1007 [107](#)  
FABS-1008 [108](#)  
FABS-1009 [108](#)  
FABS-1010 [108](#)  
FCMC-1001 [109](#)  
FCPD-1001 [109](#)  
FCPD-1002 [110](#)  
FCPD-1003 [110](#)  
FCPH-1001 [111](#)  
FKLB-1001 [111](#)  
FLOD-1001 [112](#)  
FLOD-1003 [112](#)  
FLOD-1004 [112](#)  
FLOD-1005 [113](#)  
FLOD-1006 [113](#)  
FSPF-1001 [114](#)  
FSPF-1002 [114](#)  
FSPF-1003 [114](#)  
FSPF-1005 [115](#)

FSPF-1006 [115](#)  
FSS-1001 [116](#)  
FSS-1002 [116](#)  
FSS-1003 [117](#)  
FSS-1004 [117](#)  
FSS-1005 [117](#)  
FSS-1006 [118](#)  
FSSM-1002 [118](#)  
FSSM-1003 [119](#)  
FSSM-1004 [119](#)  
FW-1001 [120](#)  
FW-1002 [120](#)  
FW-1003 [121](#)  
FW-1004 [121](#)  
FW-1005 [121](#)  
FW-1006 [122](#)  
FW-1007 [122](#)  
FW-1008 [123](#)  
FW-1009 [123](#)  
FW-1010 [124](#)  
FW-1011 [124](#)  
FW-1012 [124](#)  
FW-1033 [125](#)  
FW-1034 [125](#)  
FW-1035 [126](#)  
FW-1036 [126](#)  
FW-1037 [126](#)  
FW-1038 [127](#)  
FW-1039 [127](#)  
FW-1040 [128](#)  
FW-1041 [128](#)  
FW-1042 [128](#)  
FW-1043 [129](#)  
FW-1044 [129](#)  
FW-1045 [130](#)  
FW-1046 [130](#)  
FW-1047 [131](#)  
FW-1048 [131](#)  
FW-1049 [131](#)  
FW-1050 [132](#)  
FW-1051 [132](#)  
FW-1052 [133](#)  
FW-1113 [133](#)  
FW-1114 [133](#)  
FW-1115 [134](#)  
FW-1116 [134](#)  
FW-1117 [135](#)  
FW-1118 [135](#)  
FW-1119 [136](#)  
FW-1120 [136](#)  
FW-1121 [137](#)  
FW-1122 [137](#)  
FW-1123 [138](#)  
FW-1124 [138](#)  
FW-1125 [138](#)  
FW-1126 [139](#)  
FW-1127 [140](#)  
FW-1128 [140](#)  
FW-1129 [141](#)

FW-1130	141	FW-1244	168
FW-1131	142	FW-1245	168
FW-1132	142	FW-1246	168
FW-1133	142	FW-1247	169
FW-1134	143	FW-1248	169
FW-1135	143	FW-1249	170
FW-1136	144	FW-1250	170
FW-1137	144	FW-1251	171
FW-1138	144	FW-1272	171
FW-1139	145	FW-1273	171
FW-1140	145	FW-1274	172
FW-1141	146	FW-1275	172
FW-1142	146	FW-1296	173
FW-1143	146	FW-1297	173
FW-1144	147	FW-1298	174
FW-1160	147	FW-1299	174
FW-1161	148	FW-1300	175
FW-1162	148	FW-1301	175
FW-1163	149	FW-1302	175
FW-1164	149	FW-1303	176
FW-1165	150	FW-1304	176
FW-1166	150	FW-1305	177
FW-1167	151	FW-1306	177
FW-1168	151	FW-1307	178
FW-1169	151	FW-1308	178
FW-1170	152	FW-1309	178
FW-1171	152	FW-1310	179
FW-1172	153	FW-1311	179
FW-1173	153	FW-1312	180
FW-1174	154	FW-1313	180
FW-1175	154	FW-1314	180
FW-1176	154	FW-1315	181
FW-1177	155	FW-1316	181
FW-1178	155	FW-1317	182
FW-1179	156	FW-1318	182
FW-1180	156	FW-1319	182
FW-1181	157	FW-1320	183
FW-1182	157	FW-1321	183
FW-1183	157	FW-1322	184
FW-1184	158	FW-1323	184
FW-1185	158	FW-1324	185
FW-1186	159	FW-1325	185
FW-1187	159	FW-1326	185
FW-1188	160	FW-1327	186
FW-1189	160	FW-1328	186
FW-1190	160	FW-1329	187
FW-1191	161	FW-1330	187
FW-1192	161	FW-1331	188
FW-1193	162	FW-1332	188
FW-1194	162	FW-1333	188
FW-1195	163	FW-1334	189
FW-1216	164	FW-1335	189
FW-1217	164	FW-1336	190
FW-1218	165	FW-1337	190
FW-1219	165	FW-1338	191
FW-1240	166	FW-1339	191
FW-1241	166	FW-1340	192
FW-1242	167	FW-1341	192
FW-1243	167	FW-1342	192

FW-1343 [193](#)  
FW-1344 [193](#)  
FW-1345 [194](#)  
FW-1346 [194](#)  
FW-1347 [195](#)  
FW-1348 [195](#)  
FW-1349 [196](#)  
FW-1350 [196](#)  
FW-1351 [197](#)  
FW-1352 [197](#)  
FW-1353 [198](#)  
FW-1354 [198](#)  
FW-1355 [199](#)  
FW-1356 [199](#)  
FW-1357 [200](#)  
FW-1358 [200](#)  
FW-1359 [201](#)  
FW-1360 [201](#)  
FW-1361 [201](#)  
FW-1362 [202](#)  
FW-1363 [202](#)  
FW-1364 [203](#)  
FW-1365 [203](#)  
FW-1366 [203](#)  
FW-1367 [204](#)  
FW-1368 [204](#)  
FW-1369 [205](#)  
FW-1370 [205](#)  
FW-1371 [206](#)  
FW-1372 [206](#)  
FW-1373 [207](#)  
FW-1374 [207](#)  
FW-1375 [208](#)  
FW-1376 [208](#)  
FW-1377 [209](#)  
FW-1378 [209](#)  
FW-1379 [210](#)  
FW-1400 [210](#)  
FW-1401 [211](#)  
FW-1402 [211](#)  
FW-1403 [211](#)  
FW-1424 [212](#)  
FW-1425 [212](#)  
FW-1426 [213](#)  
FW-1427 [213](#)  
FW-1428 [213](#)  
FW-1429 [214](#)  
FW-1430 [214](#)  
FW-1431 [215](#)  
FW-1432 [215](#)  
FW-1433 [215](#)  
FW-1434 [216](#)  
FW-1435 [216](#)  
FW-1436 [217](#)  
FW-1437 [217](#)  
FW-1438 [218](#)  
FW-1439 [218](#)  
FW-1440 [218](#)  
FW-1441 [219](#)

FW-1442 [219](#)  
FW-1443 [220](#)  
FW-1444 [220](#)

## G

gathering information about the problem [37](#)  
getting help [21](#)

## H

HAM-1001 [220](#)  
HAM-1002 [221](#)  
HAM-1004 [221](#)  
HAM-1005 [222](#)  
HAMK-1001 [222](#)  
HAMK-1002 [223](#)  
HAMK-1003 [223](#)  
HIL-1101 [224](#)  
HIL-1102 [224](#)  
HIL-1103 [224](#)  
HIL-1104 [225](#)  
HIL-1105 [225](#)  
HIL-1106 [226](#)  
HIL-1107 [226](#)  
HIL-1108 [227](#)  
HIL-1201 [227](#)  
HIL-1202 [228](#)  
HIL-1203 [228](#)  
HIL-1204 [229](#)  
HIL-1205 [229](#)  
HIL-1206 [230](#)  
HIL-1301 [230](#)  
HIL-1302 [230](#)  
HIL-1303 [231](#)  
HIL-1304 [231](#)  
HIL-1305 [232](#)  
HIL-1306 [232](#)  
HIL-1307 [232](#)  
HIL-1308 [233](#)  
HIL-1309 [233](#)  
HIL-1401 [233](#)  
HIL-1402 [234](#)  
HIL-1403 [234](#)  
HIL-1404 [234](#)  
HIL-1501 [235](#)  
HIL-1502 [235](#)  
HIL-1503 [236](#)  
HIL-1504 [236](#)  
HIL-1505 [237](#)  
HIL-1506 [237](#)  
HIL-1507 [238](#)  
HIL-1508 [238](#)  
HIL-1509 [239](#)  
HIL-1601 [239](#)  
HIL-1602 [240](#)  
HLO-1001 [240](#)  
HLO-1002 [241](#)  
HLO-1003 [241](#)  
HMON-1001 [242](#)  
HP

authorized reseller [21](#)  
storage web site [21](#)  
technical support [21](#)  
HTTP-1001 [242](#)

## K

KSWD-1003 [243](#)  
KTRC-1001 [243](#)  
KTRC-1002 [243](#)  
KTRC-1003 [244](#)  
KTRC-1004 [244](#)

## L

LOG-1000 [245](#)  
LOG-1001 [245](#)  
LOG-1002 [245](#)  
looking up a system message [37](#)  
LSDB-1001 [246](#)  
LSDB-1002 [246](#)  
LSDB-1003 [247](#)  
LSDB-1004 [247](#)

## M

message severity levels [29](#)  
MPTH-1001 [248](#)  
MPTH-1002 [248](#)  
MPTH-1003 [248](#)  
MQ-1004 [249](#)  
MS-1001 [250](#)  
MS-1002 [250](#)  
MS-1003 [251](#)  
MS-1004 [252](#)  
MS-1005 [252](#)  
MS-1006 [253](#)  
MS-1007 [253](#)  
MS-1008 [254](#)  
MS-1021 [254](#)

## N

NBFS-1001 [255](#)  
NBFS-1002 [255](#)  
NBFS-1003 [256](#)  
NS-1001 [257](#)  
NS-1002 [257](#)  
NS-1003 [258](#)  
NS-1004 [258](#)

## O

overview of the system messages [29](#)

## P

panic dump files [31](#)  
PDM-1001 [259](#)  
PDM-1002 [259](#)  
PDM-1003 [259](#)  
PDM-1004 [260](#)  
PDM-1005 [260](#)  
PDM-1006 [261](#)

PDM-1007 [261](#)  
PDM-1008 [262](#)  
PDM-1009 [262](#)  
PDM-1010 [262](#)  
PDM-1011 [263](#)  
PDM-1012 [263](#)  
PDM-1013 [264](#)  
PDM-1014 [264](#)  
PDM-1017 [264](#)  
PDM-1019 [265](#)  
PDM-1020 [265](#)  
PDM-1021 [266](#)  
PDTR-1001 [266](#)  
PDTR-1002 [267](#)  
PLAT-1000 [267](#)  
Port Logs [31](#)  
PORT-1003 [268](#)  
PORT-1004 [268](#)  
PS-1000 [269](#)  
PS-1001 [269](#)  
PS-1002 [269](#)  
PS-1003 [270](#)  
PS-1004 [270](#)  
PS-1005 [271](#)  
PSWP-1001 [271](#)  
PSWP-1002 [271](#)  
PSWP-1003 [272](#)  
PSWP-1004 [272](#)

## R

RCS-1001 [273](#)  
RCS-1002 [273](#)  
RCS-1003 [273](#)  
RCS-1004 [274](#)  
RCS-1005 [274](#)  
RCS-1006 [275](#)  
reading a system message [34](#)  
related documentation [19](#)  
responding to a system message [37](#)  
RPCD-1001 [275](#)  
RPCD-1002 [276](#)  
RPCD-1003 [276](#)  
RPCD-1004 [276](#)  
RPCD-1005 [277](#)  
RPCD-1006 [277](#)  
RPCD-1007 [278](#)  
RTWR-1001 [278](#)  
RTWR-1002 [278](#)

## S

SCN-1001 [279](#)  
SEC-1001 [280](#)  
SEC-1002 [281](#)  
SEC-1003 [281](#)  
SEC-1005 [282](#)  
SEC-1006 [282](#)  
SEC-1007 [283](#)  
SEC-1008 [283](#)  
SEC-1009 [283](#)

SEC-1016	284	SEC-1093	309
SEC-1022	284	SEC-1094	309
SEC-1024	285	SEC-1095	309
SEC-1025	285	SEC-1096	310
SEC-1026	285	SEC-1097	310
SEC-1028	286	SEC-1098	311
SEC-1029	286	SEC-1099	311
SEC-1030	287	SEC-1100	311
SEC-1031	287	SEC-1101	312
SEC-1032	288	SEC-1102	312
SEC-1033	288	SEC-1104	313
SEC-1034	288	SEC-1105	313
SEC-1035	289	SEC-1106	314
SEC-1036	289	SEC-1107	314
SEC-1037	290	SEC-1108	314
SEC-1038	290	SEC-1110	315
SEC-1040	291	SEC-1111	315
SEC-1041	291	SEC-1112	316
SEC-1042	291	SEC-1115	316
SEC-1043	292	SEC-1116	316
SEC-1044	292	SEC-1117	317
SEC-1045	293	SEC-1118	317
SEC-1046	293	SEC-1119	318
SEC-1049	293	SEC-1121	318
SEC-1050	294	SEC-1122	318
SEC-1051	294	SEC-1123	319
SEC-1052	295	SEC-1124	319
SEC-1053	295	SEC-1126	320
SEC-1054	296	SEC-1130	320
SEC-1055	296	SEC-1135	320
SEC-1056	297	SEC-1136	321
SEC-1057	297	SEC-1137	321
SEC-1059	297	SEC-1138	322
SEC-1062	298	SEC-1139	322
SEC-1063	298	SEC-1142	323
SEC-1064	299	SEC-1145	323
SEC-1065	299	SEC-1146	324
SEC-1069	299	SEC-1153	324
SEC-1071	300	SEC-1154	324
SEC-1072	300	SEC-1155	325
SEC-1073	301	SEC-1156	325
SEC-1074	301	SEC-1157	326
SEC-1075	301	SEC-1158	326
SEC-1076	302	SEC-1159	326
SEC-1077	302	SEC-1160	327
SEC-1078	303	SEC-1163	327
SEC-1079	303	SEC-1164	328
SEC-1080	303	SEC-1165	328
SEC-1081	304	SEC-1166	328
SEC-1082	304	SEC-1167	329
SEC-1083	305	SEC-1168	329
SEC-1084	305	SEC-1170	330
SEC-1085	306	SEC-1171	330
SEC-1086	306	SEC-1172	331
SEC-1088	306	SEC-1173	331
SEC-1089	307	SEC-1174	331
SEC-1090	307	SEC-1175	332
SEC-1091	308	SEC-1176	332
SEC-1092	308	SEC-1180	333

SEC-1181 [333](#)  
 SEC-1182 [333](#)  
 SEC-1183 [334](#)  
 SEC-1184 [334](#)  
 SEC-1185 [334](#)  
 SEC-1186 [335](#)  
 SEC-1187 [335](#)  
 SEC-1188 [336](#)  
 SEC-1189 [336](#)  
 SEC-1190 [337](#)  
 SEC-1191 [337](#)  
 SEC-1192 [338](#)  
 SEC-1193 [338](#)  
 SEC-1194 [338](#)  
 SEC-1195 [339](#)  
 SEC-1196 [339](#)  
 SEC-1197 [340](#)  
 SEC-1198 [340](#)  
 SEC-1199 [341](#)  
 SEC-1200 [341](#)  
 SEC-1201 [342](#)  
 SEC-1202 [342](#)  
 SEC-1250 [343](#)  
 SEC-1251 [343](#)  
 SEC-1253 [343](#)  
 SEC-1300 [344](#)  
 SEC-1301 [344](#)  
 SEC-1302 [345](#)  
 SEC-1303 [345](#)  
 SEC-1304 [345](#)  
 SEC-1305 [346](#)  
 SEC-1306 [346](#)  
 SEC-1307 [347](#)  
 SEC-1308 [347](#)  
 SEC-3001 [348](#)  
 SEC-3002 [348](#)  
 SEC-3003 [349](#)  
 SEC-3004 [349](#)  
 SEC-3005 [350](#)  
 SEC-3006 [350](#)  
 SEC-3007 [351](#)  
 SEC-3008 [351](#)  
 SEC-3009 [351](#)  
 SEC-3010 [352](#)  
 SEC-3011 [352](#)  
 SEC-3012 [353](#)  
 SEC-3013 [353](#)  
 SEC-3014 [354](#)  
 SEC-3015 [354](#)  
 SEC-3016 [354](#)  
 SEC-3017 [355](#)  
 security audit logging [30](#)  
 SNMP-1001 [355](#)  
 SNMP-1002 [356](#)  
 SNMP-1003 [356](#)  
 SNMP-1004 [357](#)  
 SS-1000 [357](#)  
 SS-1001 [357](#)  
 SULB-1001 [358](#)

SULB-1002 [358](#)  
 SULB-1003 [359](#)  
 SULB-1005 [359](#)  
 SULB-1006 [359](#)  
 SULB-1007 [360](#)  
 SULB-1008 [360](#)  
 SULB-1009 [361](#)  
 SULB-1010 [367](#)  
 supportSave command [32](#)  
 SWCH-1001 [367](#)  
 SWCH-1002 [368](#)  
 SWCH-1003 [368](#)  
 SWCH-1004 [369](#)  
 SWCH-1005 [369](#)  
 symbols  
     in text [20](#)  
 symbols in text [20](#)  
 SYSC-1001 [370](#)  
 SYSC-1002 [370](#)  
 SYSM-1001 [371](#), [372](#)  
 SYSM-1002 [371](#)  
 SYSM-1003 [371](#)  
 system console [32](#)  
 system logging daemon [31](#)  
 system message log (RASLog) [30](#)  
 system module descriptions [38](#)

## T

technical support, HP [21](#)  
 text symbols [20](#)  
 Trace Logs [32](#)  
 TRCE-1001 [372](#)  
 TRCE-1002 [373](#)  
 TRCE-1003 [373](#)  
 TRCE-1004 [374](#)  
 TRCE-1005 [374](#)  
 TRCE-1006 [375](#)  
 TRCE-1007 [375](#)  
 TRCE-1008 [375](#)  
 TRCE-1009 [376](#)  
 TRCE-1010 [376](#)  
 TRCE-1011 [377](#)  
 TRCK-1001 [377](#)  
 TRCK-1002 [378](#)  
 TRCK-1003 [378](#)  
 TRCK-1004 [378](#)  
 TRCK-1005 [379](#)  
 TRCK-1006 [379](#)  
 TS-1001 [380](#)  
 TS-1002 [380](#)  
 TS-1006 [381](#)

## U

UCST-1003 [381](#)  
 UCST-1007 [382](#)  
 UPTH-1001 [382](#)  
 USWD-1006 [383](#)

## V

- view or configure the system message logs [32](#)
- viewing system messages from Advanced Web Tools [35](#)
- viewing the system messages with page breaks [36](#)

## W

- WEBD-1001 [383](#)
- WEBD-1002 [384](#)
- WEBD-1003 [384](#)
- WEBD-1004 [384](#)
- WEBD-1005 [385](#)
- WEBD-1006 [385](#)
- WEBD-1007 [385](#)

## Z

- ZOLB-1001 [386](#)
- ZONE-1002 [386](#)
- ZONE-1003 [387](#)
- ZONE-1004 [387](#)
- ZONE-1005 [388](#)
- ZONE-1006 [388](#)
- ZONE-1007 [389](#)
- ZONE-1008 [389](#)
- ZONE-1010 [390](#)
- ZONE-1012 [390](#)
- ZONE-1013 [390](#)
- ZONE-1014 [391](#)
- ZONE-1015 [391](#)
- ZONE-1017 [391](#)
- ZONE-1018 [392](#)
- ZONE-1019 [392](#)
- ZONE-1022 [393](#)
- ZONE-1023 [393](#)
- ZONE-1024 [394](#)
- ZONE-1026 [394](#)
- ZONE-1027 [394](#)
- ZONE-1028 [395](#)
- ZONE-1029 [396](#)
- ZONE-1030 [396](#)